Facultad de Ingeniería

Carrera Profesional de Ingeniería de Sistemas e Informática

" DISEÑO PARA LA AUTOMATIZACION DEL MANTENIMIENTO DE USUARIOS EN EL PROCESO DE CESES Y LA REDUCCION DEL RIESGO DE FUGA DE INFORMACION EN EL BANCO FINANCIERO DEL PERU"

Autor: Jorge Joel Acosta Panduro

Para obtener el Título Profesional de

Ingeniero de Sistemas e Informática

Asesor: Víctor Enrique Quevedo Dioses

Lima, diciembre 2018

Este trabajo está dedicado a mis padres ***Jorge Acosta Vílchez y Magdalena Panduro Cueva****, quienes desde niño siempre me inculcaron el amor al estudio, al prójimo y que no existe barreras cuando uno tiene las ganas y la convicción de realizarlas.*

AGRADECIMIENTO

A Dios como fuente universal de amor, quien me otorgo sabiduría para tomas las decisiones correctas y fortaleza para derrotar cualquier obstáculo.

A todas aquellas personas que constantemente me daban aliento para poder culminar esta etapa, a mis Hermanos Diego Alberto Acosta y Marco Antonio Acosta, a mi amigo Miguel Solano y familiares.

A mi esposa Úrsula Vizarreta Pacheco, que es mi soporte emocional y en esos días donde el cansancio pesaba sobre la espalda, sus palabras eran la fuerza para continuar.

RESUMEN

Actualmente vivimos en un mundo de constantes cambios tecnológicas y aquellas Organizaciones que no estén preparadas para enfrentar este reto simplemente están condenadas al fracaso devoradas por la competencia. La seguridad Informática no debe ser considerado como un ente aislado que brinda soporte a los procesos de negocio, sino como factor clave dentro del plan estratégico de las empresas.

La migración de las plataformas tecnológicas de un entorno On Premise hacia Tecnologías Cloud o Nube no es una moda y está en crecimiento, cada vez las Organizaciones del sector financiero están obligadas a cambiar la arquitectura de sus servicios para adaptarse al mercado y buscar la innovación sobre los diferentes productos que se brindan a los clientes.

Tanto el proceso de Selección para nuevos ingresos **[PROCESO DE ALTAS**] y el proceso de Cese de Labores [**PROCESO DE CESE**] de colaboradores en una entidad financiera, siguen estándares Basadas en las Best Practices de Seguridad de Información ISO 27001 cuyo fin es mantener la triada de la seguridad: Integridad, Confidencialidad y **Disponibilidad**.

La disponibilidad involucra que los usuarios tengan acceso a las aplicaciones que corresponda según su perfil dentro de la empresa y de igual forma restringir los accesos cuando el colaborador sea cambiado de cargo o deje de laborar en la institución, estas tareas actualmente se ejecutan de **forma Manual** en el Banco Financiero lo que provoca:

1. Esfuerzo elevado de Horas/Hombre en tareas Operativas.
2. Errores Manuales al momento de ejecutar los Ceses.
3. Accesos no Autorizados por préstamo de Credenciales.
4. Observaciones de Auditoría por cuentas huérfanas.
5. Margen elevado entre la fecha de Cese y el retiro de los accesos.

.

Es por ello que el presente trabajo de investigación, propone un nuevo modelo de servicio del área de Control de Accesos perteneciente a Seguridad Informática, orientado al diseño de la automatización del Proceso de Ceses y cuyo alcance es sobre las aplicaciones que el Banco Financiero a ha identificado críticas para el Negocio.

El presente trabajo de investigación estará estructurado en 4 capítulos: El Capitulo #1 detallará el planteamiento de la problemática actual, los objetivos en el orden general y específicos, las Hipótesis y Justificación de la Investigación.

El Capítulo #2 se desarrollará el Fundamento Teórico, donde se describirá todos los estándares, tecnologías y conceptos relevantes para la investigación. También se plantea la metodología que se fijará para el cumplimiento de los Objetivos Planteados.

En el Capítulo #3 se Desarrollará la propuesta del Nuevo Diseño del Proceso de Ceses orientado hacia la automatización de tareas manuales dentro del Macro Proceso. Finalmente, en el Capítulo #4 realizaremos el análisis de Costo y Beneficio para confirmar la viabilidad del Proyecto.

SUMMARY

We currently live in a world of constant technological changes and those Organizations that are not prepared to face this challenge are simply doomed to failure devoured by competition. Computer security should not be considered as an isolated entity that provides support to business processes, but as a key factor in the strategic plan of companies.

The migration of the technological platforms of an On Premise environment towards Cloud or Cloud Technologies is not a fad and is growing, every time the financial sector Organizations are obliged to change the architecture of their services to adapt to the market and seek innovation over the different products that are offered to customers.

Both the selection process for new revenues [ALTAS PROCESS] and the process of cessation of work [CESE PROCESS] of collaborators in a financial institution, follow standards based on the Best Practices of Information Security ISO 27001 whose purpose is to maintain the triad of security: Integrity, Confidentiality and Availability.

Availability implies that users have access to the corresponding applications according to their profile within the company and in the same way restrict access when the employee is changed or leaves work in the institution, these tasks are currently executed manually in Banco Financiero, which causes:

1. High Hours / Man effort in operational tasks.
2. Manual Errors when executing the Ceses.
3. Unauthorized Access by Loan of Credentials.
4. Audit observations for orphan accounts.
5. High margin between the date of cessation and withdrawal of access.

.

That is why this research work, proposes a new service model in the area of Access Control belonging to IT Security, aimed at the design of the Ceses Process automation and whose scope is on the applications that Banco Financiero has identified critical to the Business.

The present research work will be structured in 4 chapters: Chapter # 1 will detail the approach of the current problem, the objectives in the general and specific order, the Hypothesis and Justification of the Research.

Chapter # 2 will develop the Theoretical Foundation, which will describe all the standards, technologies and concepts relevant to research. It also considers the methodology that will be set for the fulfillment of the Objectives.

In Chapter # 3 will be developed the proposal of the New Design Ceses Process oriented towards the automation of manual tasks within the Macro Process. Finally, in Chapter # 4 we will perform the Cost and Benefit analysis to confirm the viability of the Project.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCION

Actualmente vivimos en un mundo que cambia constantemente y las nuevas tecnologías hacen cada día más sencilla la transferencia y tratamiento de información en todas sus formas. La información como tal, constituye un activo crítico para las empresas y en el caso de las empresas del sector financiero resulta aún más sensible puesto que engloban Data de Clientes asociadas a cuentas Bancarias, tarjetas de Crédito, etc.

Según el Portal **Identity Theft Resource Center** informó que en el 2014 en Estados Unidos se detectaron 1´198,492 registros de información relacionados a Incidentes de Fuga de Información en el sector Bancario. En este contexto, la fuga de información corresponde uno de los riesgos más devastadores para un Banco, involucra pérdida de dinero y sobre todo reputación

Es por ello que los controles de Seguridad que deben implementar los Bancos deben estar enfocados no solo en los sistemas, sino también en las personas que son la pieza más frágil de la seguridad y en **los Procesos**. El Banco Financiero del Perú tiene implementado un SGSI y como parte de sus controles de Seguridad alineados a la ISO 27002 (Buenas Prácticas de Seguridad de Información), existe un Procedimiento para el Proceso de Ceses de Usuarios.

En el presente trabajo de investigación abordaremos la mejora del mantenimiento de Usuarios en el Proceso de Ceses del Banco Financiero. Esta actividad en la actualidad se realiza de forma manual y se propone un nuevo diseño orientado a la automatización de algunas tareas. En el capítulo 3, se detalla la forma de automatización para las 4 aplicaciones críticas que ha considerado el negocio, así como también los beneficios que se obtendrían al implementarse el nuevo diseño.

CAPITULO 1

ASPECTOS GENERALES

1. ASPECTOS GENERALES

1.1. INFORMACION PRELIMINAR

1.1.1. Información de la Empresa

El Banco Financiero inicia sus actividades en el Perú en el año 1964 con el nombre de **FINANCIERA Y PROMOTORA DE LA CONSTRUCCION S.A**, posteriormente en el año 1982 cambia de nombre a **FINANPRO** Empresa del rubro Finanzas.

El 21/11/1986 se constituye con el nombre comercial de **BANCO FINANCIERO**.

En el año 2001 el BANCO FINANCIERO compra el NBK Bank , con lo cual consolidada su ampliación el mercado peruano . También promueve la diversificación de sus productos y carteras de negocio, dado que en el pasado estuvo concentrado solo en el sector empresarial. El BFP desarrolla operaciones bancarias de consumo, microcrédito y a partir del año 2004 se expandieron en la entrega de créditos a través de los llamados convenios.

Actualmente el Banco Financiero tiene firmadas alianzas estratégicas con Grupos de Negocio como CARSA, Diners Club, Diners Travel, Amerika Financiera y Crecer Seguros, con un universo de empleados que asciendo aproximadamente a 1800 usuarios en sus casi 70 agencias a nivel nacional.

Estos son los canales de atención del Banco Financiero:

- ✓ Red de Agencias ›
- ✓ Banca Telefónica ›
- ✓ Banca por Internet ›
- ✓ Saldomático ›

- ✓ Red de Cajeros Globalnet ›
- ✓ Banca Celular ›
- ✓ Agentes Corresponsales ›
- ✓ Billetera Móvil ›

1.1.2. Misión

Impulso del crecimiento sostenible de sus clientes, sus colaboradores, accionistas y del país.

1.1.3. **Visión**

Su visión es Ser el Banco líder en ofrecer soluciones financieras a su mercado objetivo, brindando calidad en su servicio, eficiencia y oportunidad

1.1.4. Valores Corporativos

Orientación al cliente:

- Satisfacer las necesidades de sus clientes en base al conocimiento de los mismos
- Transparencia y Simplicidad en las operaciones.
- Cercanía y Disponibilidad
- Amabilidad

Orientación a las Personas:

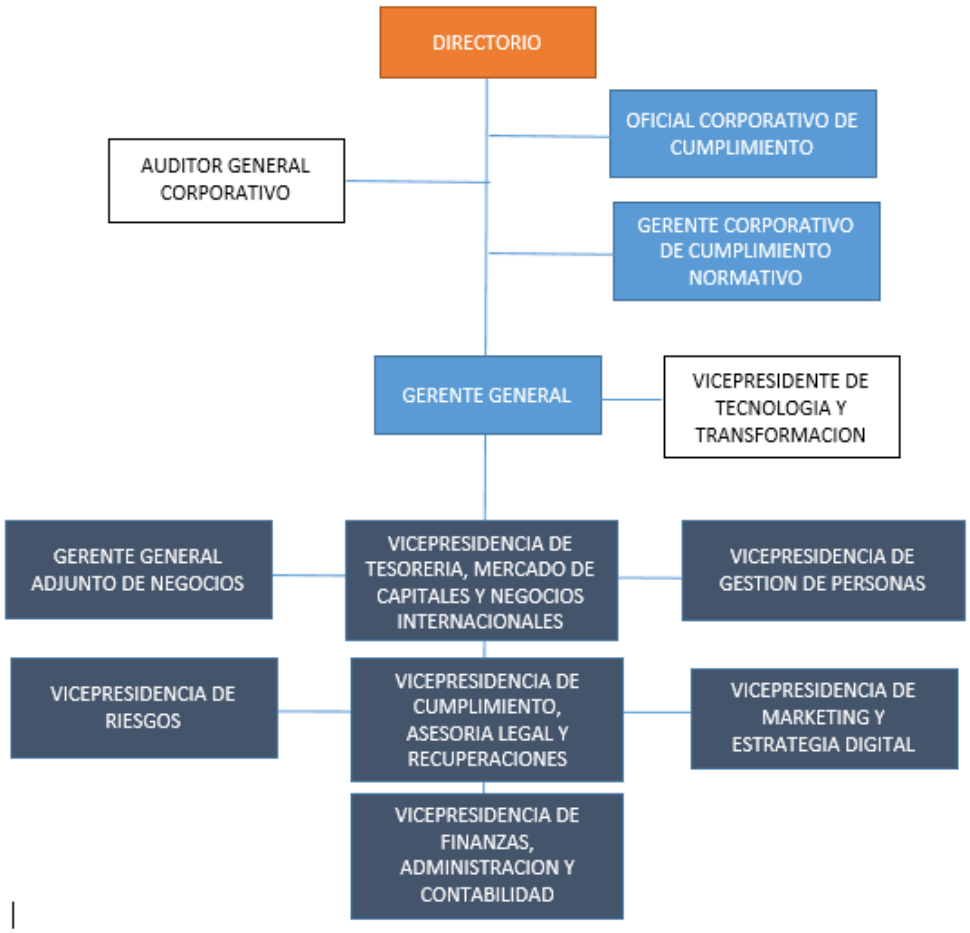
- Confianza
- Equidad
- Reconocimiento y desarrollo
- Trabajo en equipo

Orientación al Logro

- Visión global
- Integridad
- Proactividad
- Responsabilidad y compromiso

1.1.5. Organigrama

Figura N° 1 : Organigrama del Banco Financiero del Perú



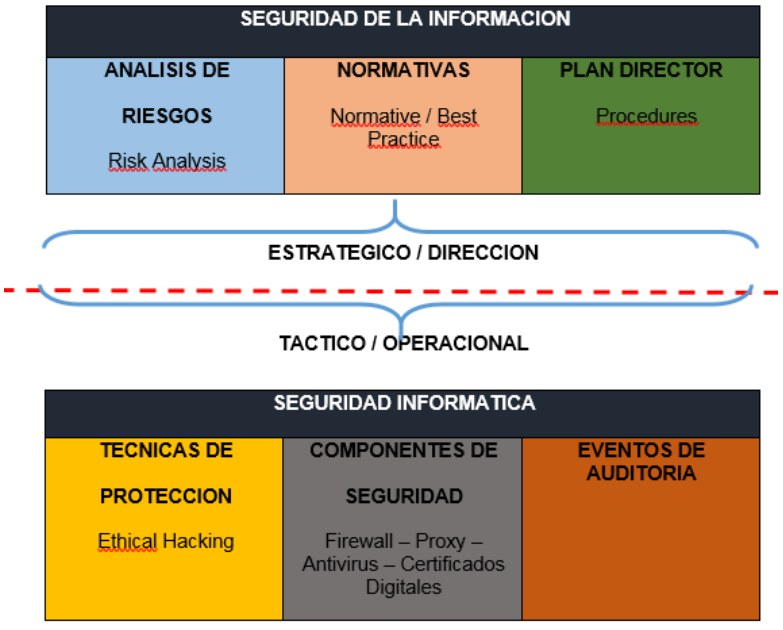
Fuente: Elaboración Propia

1.2. DEFINICION DEL PROBLEMA

1.2.1. DESCRIPCION DEL PROBLEMA

La información constituye uno de los activos más importantes para una empresa y en el sector financiero resulta crítico dado que maneja Data sensible en grandes volúmenes y en donde podemos encontrar: Números de tarjetas de crédito, Débito, Productos Hipotecarios, Prestamos PLD etc. Es por ello que los Bancos están sujetos a rigurosas auditorías internas y externas por entes regulatorios SBS, quienes deben certificar que la entidad este cumplimiento con los Estándares Internacionales [**ASA, PCI, ISO 27001**] para el manejo de la Información. El Banco Financiero del Perú tiene implementado un SGSI [Sistema de Gestión de Seguridad de Información] y en donde existen dos áreas que trabajan diariamente para la continuidad del Sistema:

Figura N° 2 : Diagrama Interacción Seguridad TI – Seguridad de Información



Fuente: Elaboración Propia

El SGSI implementado en el Banco Financiero está alineado a la norma técnica ISO/IEC 27002:2013 y en el dominio **A.9 CONTROL DE ACCESOS/Objetivos de Control *9.2.- Gestion de Accesos de Usuario. /Control 9.2.1.- Registro y Baja de Usuario***

Este control tiene como responsables Operativos de la ejecución al área de Control de Accesos – Seguridad Informática y que actualmente se encuentra como Outsourcing

Tenemos un procedimiento de Aprovisionamiento y Baja de Accesos Informáticos, el cual **se ejecuta de forma manual** y que consiste en acceder al módulo de Seguridad de cada aplicación, de acuerdo a la matriz de perfilamiento se ejecuta la baja del usuario. El BFP tiene aproximadamente 60 aplicaciones que son administradas y el tiempo promedio para ejecutar un Cese de Usuario es aproximadamente 30 minutos. El margen de tiempo entre la notificación de Cese y Ejecución del mismo, genera un espacio en el cual el usuario podría usar distintos medios digitales: Correo, USB, Bluetooh, Tarjeta SD Lectora, páginas de carga de información On Line, Etc. para que de forma indiscriminada pueda extraer la información del Banco Financiero.

En base a lo expuesto, para este presente estudio se ha identificado la siguiente problemática **‘’Riesgo Elevado de Fuga de Información por Usuarios Cesados¨.** La información como activo crítico del Banco Financiero debe ser protegida y de no tomar acciones inmediatas estará expuesto a sufrir Fraudes Financieros que afectarían su reputación, confianza de los clientes y perdida de millones. Adicional a ello también el Banco Financiero está sujeto a sanciones penales y la no renovación de Estándares (ASA, PCI,ect) que son auditados cada cierto tiempo en Base al cumplimiento de los Objetivos.

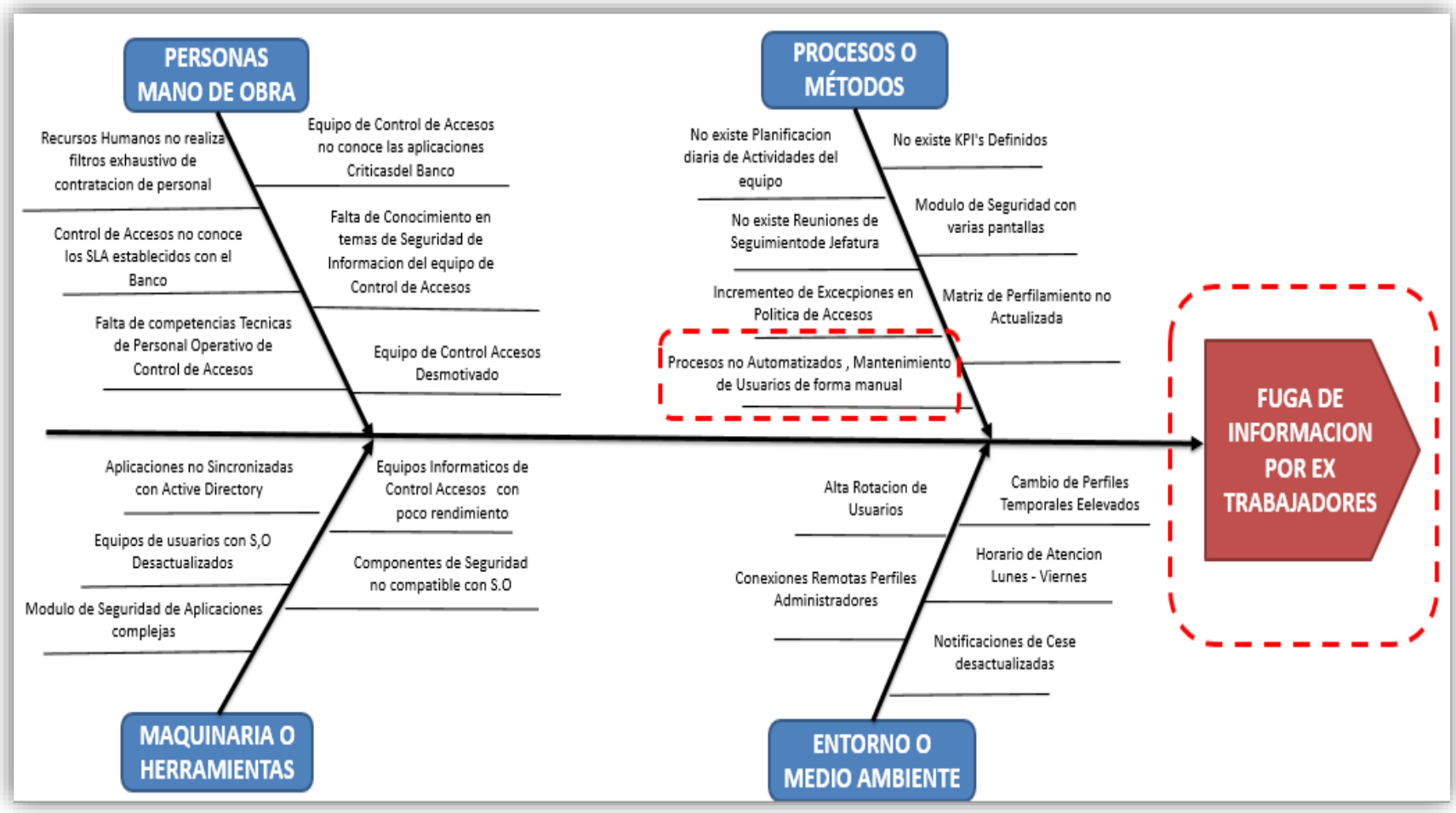
El problema planteado tiene múltiples posibles causas, sin embargo, para esta investigación se plantea que la causa principal es el alto esfuerzo de **horas/hombre** que se invierte por cada Cese de Usuario al tratarse de actividades manuales-operativas.

Dentro del presupuesto anual del Banco Financiero no se tiene presupuestado la adquisición de un software de Gestión de Identidades [IAM] por el alto costo que implica. Esto nos exige a plantear alternativas cuya implementación no generen una inversión alta, utilizando los recursos actuales tanto **Software/Hardware/Personas** orientados a la automatización.

Como solución a la Problemática planteada se propone un diseño que implica automatizar el Mantenimiento de Usuarios correspondiente al Proceso de Ceses sobre las Aplicaciones que el Banco Financiero considera Criticas, centralizando la Base de usuarios Cesados en una sola Fuente desde donde cada aplicación a través .de una tarea programada ejecutará de forma automática las Bajas y con ello mitigando el riesgo de fuga de información.

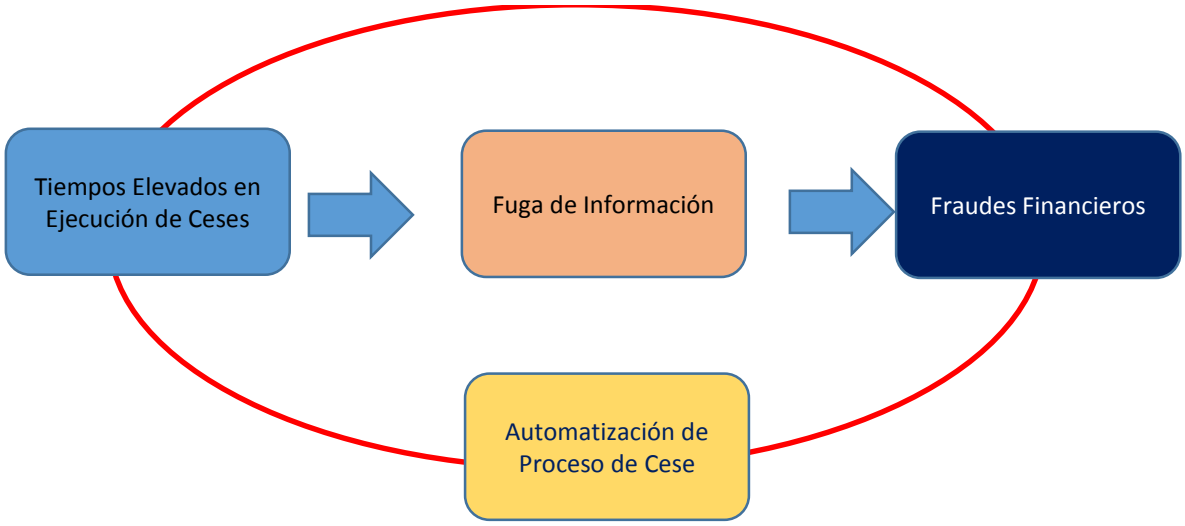
A continuación, mostramos un diagrama de Ishikawa donde podemos apreciar gráficamente los distintos factores adyacentes al problema planteado:

Figura N° 3 : Diagrama de Ishikawa – Identificación del Problema



Fuente: Elaboración Propia

Figura N° 4 : Esquema de Formulación del Problema



Fuente: Elaboración Propia

1.3. FORMULACION DEL PROBLEMA

En esta sección se presenta la formulación del problema general y la formulación de los problemas específicos.

1.3.1. Formulación del problema general

¿El diseño de la automatización del mantenimiento de usuarios en el Proceso de Ceses en el Banco Financiero reducirá el riesgo de fuga de información?

1.3.2. Formulación de problema específico 1

¿El diseño de la automatización del mantenimiento de usuarios en el Proceso de Ceses en el Banco mejorará la eficiencia en tiempos de ejecución de las Bajas?

1.3.3. Formulación de problema específico 2

¿El diseño de a automatización del mantenimiento de usuarios en el Proceso de Ceses en el Banco reducirá la carga operativa del equipo de Control de Accesos?

1.3.4. Formulación de problema específico 3

¿El diseño de la automatización del mantenimiento de usuarios en el Proceso de Ceses en el Banco reducirá errores manuales.?

1.4. DEFINICION DE OBJETIVOS

1.4.1. Objetivo General

Diseñar la automatización del mantenimiento de usuarios en el Proceso de Ceses en el Banco Financiero para reducir el riesgo de fuga de información

1.4.2. Objetivo Especifico 1

Diseñar la automatización del mantenimiento de usuarios en el Proceso de Ceses en el Banco Financiero para mejorar la eficiencia en tiempos de ejecución de las Bajas

1.4.3. Objetivo Especifico 2

Diseñar la automatización del mantenimiento de usuarios en el Proceso de Ceses en el Banco Financiero para reducir la carga operativa en el equipo de Control de Accesos

1.4.4. Objetivo Especifico 3

Diseñar la automatización del mantenimiento de usuarios en el Proceso de Ceses en el Banco Financiero para reducir errores manuales

1.5. HIPOTESIS

1.5.1. Hipótesis General

El diseño de la automatización del mantenimiento de usuarios en el Proceso de Ceses en el Banco Financiero reduce el riesgo de fuga de información

1.5.2. Hipótesis Especifica 1

El diseño de la automatización del mantenimiento de usuarios en el Proceso de Ceses en el Banco mejorará la eficiencia del Servicio de Ceses.

1.5.3. Hipótesis Especifica 2

El diseño de la automatización del mantenimiento de usuarios en el Proceso de Ceses en el Banco reducirá la carga operativa del equipo de Control de Accesos.

1.5.4. Hipótesis Especifica 3

El diseño de la automatización del mantenimiento de usuarios en el Proceso de Ceses en el Banco reducirá errores manuales.

1.6. JUSTIFICACION DE LA INVESTIGACION

El Banco Financiero del Perú actualmente tiene implementada una Política de Control de Accesos y del cual se desprende los Procedimientos para la Altas/Ceses de Usuarios, sin embargo, al no contar con procesos automatizados que simplifiquen estas tareas se convierte en una actividad 100% manual.

La operativa trae como resultado errores, inversión de tiempo horas/hombre muy elevadas y esta brecha de tiempo entre la notificación de Cese desde Recursos Humanos hasta la ejecución por el equipo de Control de Accesos deja abierta las puertas a usuarios mal intencionados que posiblemente puedan robar información confidencial de la institución.

Es necesario plantear alternativas que minimicen la brecha de tiempo que los accesos permanecen aún activos, por ejemplo, si un Cese es notificado un día viernes después de las 04:00 pm (**SLA comprometido con el Banco**) este no será ejecutado hasta el día lunes existiendo dos días en los cuales el usuario a través de las soluciones Cloud [Correo Electrónico Exchange Online] o Soluciones VPN Citrix Remote Desktop pueda sacar información. Esto se vuelve más crítico al tratarse de perfiles con privilegios a nivel de **administrador de aplicaciones** por ejemplo usuarios de Tecnología u Operaciones.

El Banco Financiero está orientado a una política de ahorro de costos y la implementación de un Gestor de Identidades Sofisticado es un proyecto muy costoso cuyo ROI es lento, en este proyecto de estudio se plantea el diseño de la automatización de los Ceses de Usuarios sobre las aplicaciones críticas definidas por el Negocio como una solución que puede ser implementada en poco tiempo, a bajo costo y un alcance definido que no involucra cambios en la infraestructura actual.

CAPITULO 2

FUNDAMENTO TEORICO

2.1. ANTECEDENTES

2.1.1. **Jehu Benigno Martínez Cabrera (2018)** ‘’IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO A RED EN LA EMPRESA SIMA - CHIMBOTE; 2018’’

Este Proyecto de Estudio se orientó en el ámbito de la línea de investigación de las (TIC) planteando la mejora continua de la calidad de las empresas peruanas. El Bachiller de la Universidad Católica los Ángeles de Chimbote perteneciente a la escuela profesional de Ingeniería de Sistemas propone en su proyecto Implementar un sistema de control de acceso a la red corporativa de la empresa SIMA que se ubica en la ciudad Chimbote, con ello busca la mejora de la Gestión de Accesos de las cuentas de red de Usuarios y a su vez fortalecer la seguridad en la red. El diseño del Trabajo es no experimental y se cuenta con una Población de 10 usuarios internos, dado que la población es pequeña se considera la muestra como el total de usuarios. En la parte Metodológica se siguió un método no probabilístico y con muestra por conveniencia.

El Alumno desarrolló un cuestionario con preguntas centradas a la implementación del sistema de acceso a la red y se obtuvieron los siguientes resultados:

50% Empleados: Satisfechos con la Atención de Acceso a la red Actual.

50% Empleados: No Satisfechos con la Atención de Acceso a la red Actual.

Con respecto a la dimensión Necesidad de implementación de un sistema de control de acceso a red, tenemos los siguientes resultados:

100% Empleados: SÍ es necesario la implementación de un sistema de control de acceso a red. En Base a los resultados obtenidos , se puede confirmar la hipótesis general y se justifica el trabajo de investigación con el fin de implementar un sistema de control de acceso a red en la empresa SIMA – Chimbote. **(Martinez Cabrera Jehu Benigno, 2018)**

2.1.2. **Frankz Olivos Guerra y Erick William Guevara Saldaña (2017)** ‘’FORMULACIÓN DE POLÍTICAS DE CONTROL DE ACCESOS Y SEGURIDAD FÍSICA Y DEL ENTORNO BASADO EN LA NORMA TÉCNICA PERUANA NTP-ISO/IEC 17799 PARA LA MEJORA DE LA GESTIÓN EN LA OFICINA CENTRAL DE CÓMPUTO – UNIVERSIDAD DE LAMBAYEQUE’’

En el escenario actual todas las organizaciones, incluidas las que se encuentran en el sector de Educación, tienen dificultades para mantener un control efectivo sobre sus activos de información lo que conlleva a su vez riesgos sobre otro tipo de activos de la Empresa.

La presente investigación tiene como Objetivo la Formulación de Políticas de Seguridad Física y Control de accesos, para ello se utilizó una metodología de Gestión de Riesgos que fue desarrollada por los mismos autores del Trabajo de Investigación; como fuentes de información se tomó como referencia la norma peruana NTP-ISO/IEC 17799. Dentro del análisis de la problemática actual, los autores identificaron que no existen buenas prácticas para el tratamiento de la información, no se tienen políticas, normas, procedimientos implementados y esto genera un riesgo muy alto pues no se asegura los principios Básicos de la Seguridad de Información. En base a esa brecha de seguridad Identificada, los autores proponen en la presente investigación la implementación de políticas de control de accesos lógicos y de seguridad física, cuya finalidad es que los usuarios adopten estas políticas como parte de las tareas diarias para la mejora de la oficina central de Computo (OCC). También se tiene como Objetivo, con la formulación de las políticas la Organización se encuentre alineada a los estándares de seguridad de la información mundial y lo que asegurará su funcionamiento. Como resultado del trabajo de investigación, se tendrá formulada un 53% de políticas basadas en la NTP-ISO/IEC 17799. Esto generará un aumento en el grado de aprobación de la gestión de la seguridad de la información en la OCC de la UDL. **(Olivos Guerra Frankz y Guevara Saldaña William, 2017)**

2.1.3. **Karla Evita Castro Valverde y Jannet Del Rosario Guzmán Delgado (2010)** ‘’IMPLEMENTACION DEL SISTEMA DE ADMINISTRACION DE ACCESOS E IDENTIDADES EN EL PROCESO DE CONTROL DE ACCESOS’’

El Banco de la Nación tiene implementada la División de Seguridad de Información y a través de ella se centraliza la Gestión de Accesos y se genera las credenciales de acceso de las distintas aplicaciones que tiene el Banco en los Módulos de Seguridad. Para que se proceda con la creación de nuevos usuarios deberá existir una notificación formal que llega desde el Departamento de Personal a la División Seguridad de Información; este flujo de trabajo trae como consecuencia un control deficiente respecto al aprovisionamiento de accesos de los usuarios y estaría generando incumplimientos con respecto a las normativas vigentes que regulan los temas de Seguridad, un claro ejemplo la Circular SBS G-140; dada la problemática actual, existe el riesgo sobre los activos de información del BN. El Banco de la Nación actualmente tiene aproximadamente 250 aplicaciones implementadas en su red y una población total de 5,500 usuarios en todo el Perú. El objetivo principal de este trabajo de investigación es gobernar de forma eficiente los accesos a las aplicaciones del BN, para ello se propone implementar un Sistema de Gestión de Identidades y con esta implementación se tiene esperado una mejora en los controles de seguridad de los activos de información. **(Castro Valverde Karla y Guzmán Delgado Jannet Del Rosario Evita, 2010)**

2.2. MARCO TEORICO

2.2.1. Sociedad de la Información:

Es la nueva concepción de la era actual y que se considera un nuevo modelo de vida que está generando cambios significativos en la sociedad. Esta evolución está siendo inducida primariamente por los nuevos medios que se encuentran disponibles para el tratamiento de

la información en todas sus formas mediante tecnologías digitales. **(Comision Economica para America Latina y el Caribe, 2003)**

El avance acelerado de la Tecnología está trayendo cambios significados en la vida de las personas y en la percepción de las cosas Las tareas que antes se realizaban, en el ámbito laboral hoy pueden ser procesadas en algunos casos sin la intervención del hombre, la forma de comunicarse y socializar actualmente basta solo con un click en nuestro ordenador. Todo este desarrollo tiene principalmente a las TIC (Tecnologías de la Información, la Comunicación) como las Bases que lo soportan y están haciendo que la sociedad evolucione de forma agresiva, similar en línea de tiempo como se vivieron cambios radicales con otros avances en la historia del ser humano: descubrimiento del fuego , construcción de la rueda , etc. .

Figura N° 5 : Evolución de la Sociedad en el Tiempo

Fuente: Elaboración Propia

La humanidad está en dirección hacia una nueva era y nivel de desarrollo, a estos cambios las personas expertas denominado la Sociedad de la Información. Este concepto no es nuevo y ya en décadas anteriores 80’ se puede encontrar existencia de su

conceptualización y que nos describe que todo tratamiento de la información ya sea en su creación, uso, transferencia y eliminación son actualmente la razón esencial de las actividades del ser humano.

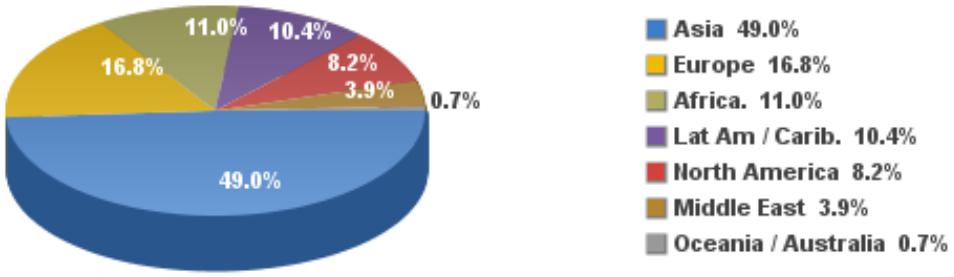
La Sociedad de la Información, tienen en sí mismo mejoras en distintas áreas del ser humano, un claro ejemplo es Internet que proporciona a las personas una herramienta única a través de la cual la información puede ser distribuida en tiempo real y entre dos puntos del planeta tierra que físicamente se encuentra a kilómetros de distancia.

Las personas para comunicarse con el resto del mundo ya no necesitan conectarse a través de una Computadora personal, sino que basta con usar su teléfono móvil, laptop o Tablet donde tienen una diversidad de aplicaciones que pueden ser descargadas. Adicional a ello las organizaciones se encuentran en la Línea de digitalizar sus servicios, esto se ha convertido más que en una moda una necesidad dada la competencia que debe adaptarse a los nuevos consumidores. De igual forma el Trabajo Remoto se ha vuelto una opción viable para las organizaciones, sin embargo, existen ciertas regulaciones que deben tenerse en cuenta.

Si bien es cierto la revolución tecnológica trae consigo una gran cantidad de beneficios, debe tenerse en cuenta que los gobiernos deben implementar normativas en el marco legal que permitan el uso de las TIC, considerando dentro de ella los riesgos que involucran y los controles a implementarse para su mitigación. De igual forma debe considerarse la implementación de programas que minimice la brecha entre las personas que tienen acceso a las TIC y aquellas que por distintos factores estén limitados.

La Sociedad de la Información ya no se trata de un concepto que esta moda, es parte de nuestra vida y se encuentra interiorizada en nuestras actividades cotidianas.

Figura N° 6 : Uso de Internet por Región



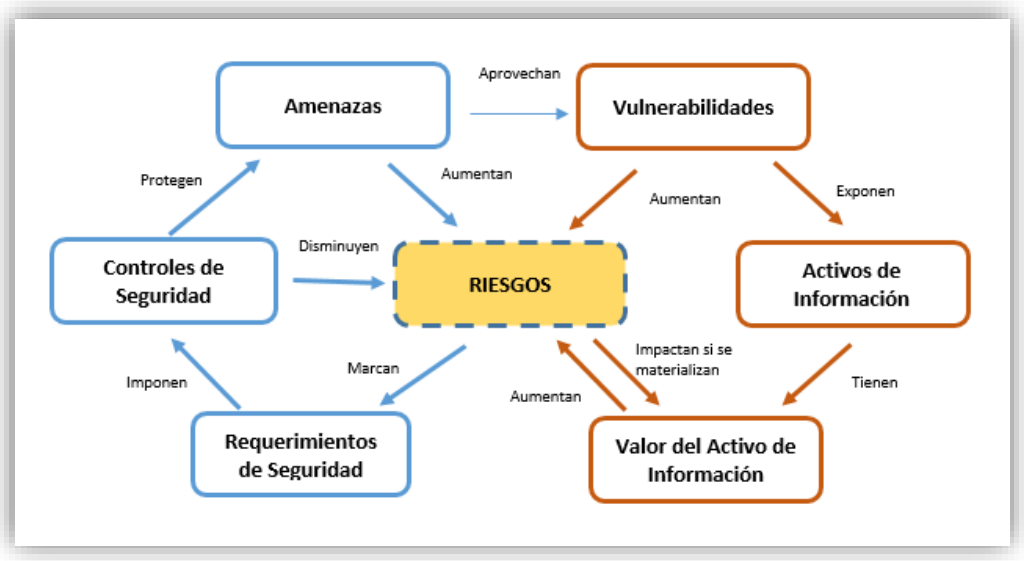
Fuente: Internet World Stats www.internetworldstats.com

2.2.2. ISMS (Information Security Management System)

Podemos definir un Sistema de Gestión de Seguridad de Información como una forma sistémica de abordar y gobernar la gestión de la Information Security empresarial para protegerla. Esto involucra tanto a las personas, procesos y sistemas informáticos.

Un SGSI, nos permite identificar los riesgos que están asociados a los activos de información de nuestra organización y los asume, minimiza, transfiere o mitigamos mediante un sistema definido, documentado y conocido por toda la organización.

Figura N° 7 : Riesgos y su interrelación con el entorno



Fuente: Elaboración Propia

2.2.3. ISO

2.2.3.1. Marco Histórico

LA ISO es un organismo cuyas siglas significan ‘"Organismo Internacional de Normalización’’ fue instituido en el año 1947 y está integrado por 91 miembros pertenecientes a los distintos estados a nivel mundial. La razón de ser de este organismo es trabajar en forma conjunta con todos los miembros para diseñar en base a las Buenas prácticas marcos de referencia en distintas áreas de trabajo. La finalidad es formalizar y establecer sistemas de calidad, que generen en el cliente final la satisfacción sobre sus expectativas.

A mediados de la década del 80’, la ISO dispuso la formación de comités integrados por personal técnicos con la finalidad de la elaboración de normas comunes y que estas sean aceptadas a nivel mundial. Luego de 7 años de trabajo se obtuvieron los primeros resultados, consolidando la publicación del compendio de las Normas ISO 9000.

El avance y perfeccionamiento de las Normas ISO en la actualidad tiene una gran relevancia en las organizaciones que buscan eficiencia en sus procesos y han ido extendiendo hacia otras áreas tales como el Medio Ambiente, Seguridad Laboral, etc.

La revisión de las normas es un proceso cíclico y constantemente van publicándose nuevas versiones de las ya existentes y nuevas normas sobre áreas que recién se han integrado.

2.2.3.2. Finalidades y ventajas de las normas ISO

Las normas ISO se desarrollaron teniendo como fin mayor unificar los criterios de expertos en base a un consenso de las mejores experiencias con resultados probados en la práctica y compartirlo con las Organizaciones para que ellas en su implementación puedan

materializar la reducción de costos y el aumento d la efectividad de sus procesos, también permite a las empresas seguir un estándar en la producción y prestación de los servicios alineados a las buenas practicas universales.

Actualmente las Normas ISO han sido adoptadas por una inmensidad de empresas a nivel mundial y con ello han homologado sus procesos de acuerdo a las directrices que se describen en cada norma. Los resultados han sido comprobados, mejorando la calidad de los servicios brindados y productos desarrollados.

2.2.3.3. Ventajas de las normas ISO para las empresas

Las siguientes ventajas expuestas, son en base a los resultados obtenidos de la implementación práctica en cada una de sus ramas Podemos enumerar las siguientes:

1. Brinda directrices a las empresas para que alcancen un nivel de calidad optimo en la producción y prestación de servicios a clientes finales.
2. Proveen las herramientas para poder brindar calidad a clientes cada vez mas exigentes.
3. Reducción de costos, Aumento de Productividad
4. Reducción en los errores operativos.
5. La mejora continua como parte esencial del Proceso.
6. Apertura puertas hacia nuevos mercados y genera mayor confianza en los clientes.

2.2.4. Familias de Normas ISO

Las Normas ISO periódicamente se van actualizando y también pueden crearse nuevas en base al consenso de los miembros integrantes. Las Normas ISO están estructuradas en Familias y cada una de ellas tiene asignada una nomenclatura.

Actualmente las Normas ISO se dividen en tres Categorías principales:

2.2.4.1. SERIE 9000 Gestión de Calidad

Estas Normas están centradas en homologar los estándares de calidad de los Servicios o Productos finales, independientemente de su naturaleza Pública – Privada, de su tamaño Grande, Mediana o pequeña o se su razón de ser.

2.2.4.2. SERIE 14000 Gestión del medio ambiente

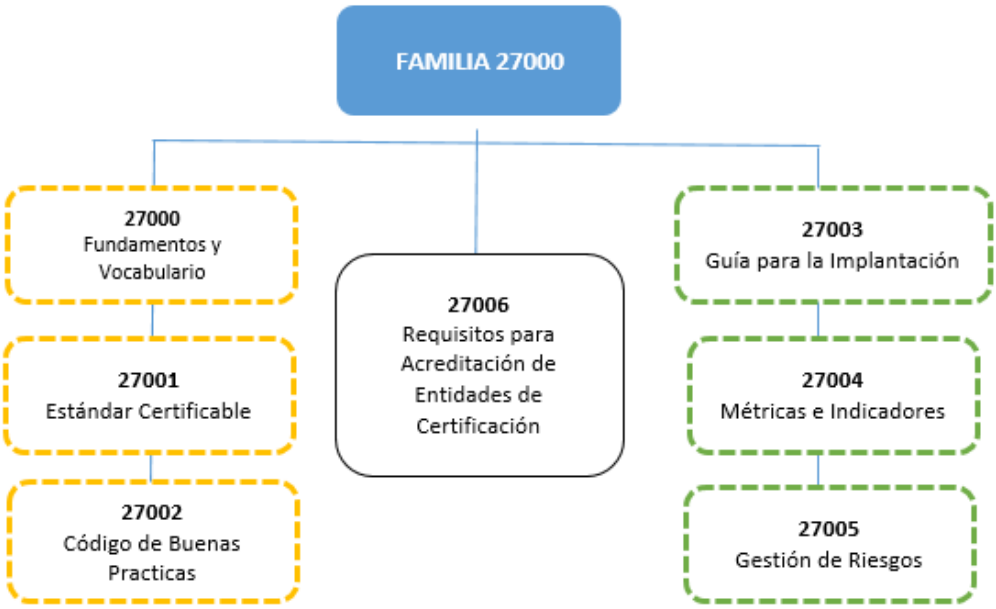
Esta Norma está orientada para que las Organizaciones puedan realizar sus actividades respetando nuestro medio ambiente o entorno natural. Para ello proporciona conocimiento sobre el cumplimiento de las normativas y marco legal actual.

2.2.4.3. Norma ISO 22000, OHSAS 18001, ISO 27001, ISO 22301 Gestión de riesgos y seguridad

Estas Normas están elaboradas para que las Empresas puedan minimizar el riesgo que está asociado a las distintas amenazas que puedan materializarse en el desempeño de las actividades empresariales en cualquiera de los rubros al que se dedique la Organización.

2.2.5. FAMILIA 27000

Figura N° 8 : ISO Familia 2700



Fuente: Elaboración Propia

2.2.5.1. ¿Cómo funciona la ISO 27001?

La razón fundamental de la Norma ISO 27001 es resguardar los 3 pilares de la Seguridad de Información: Integridad, confidencialidad y disponibilidad en las Organizaciones. Para ello se debe implementar una metodología de Gestión de Riesgo que nos permita identificar cuáles son las Amenazas más probables que afectarían nuestros activos de información, esta fase descrita es la Evaluación del Riesgo y una vez identificada las amenazas debe implementarse los controles que mitigaran, esta fase es Tratamiento del Riesgo .

En base a lo descrito anteriormente la razón de ser de la Norma ISO 27001 tienen sus principios en la Gestión de Riesgos.

Figura N° 9 : Estructura ISO27001

Fuente: 27001 Academy https://advisera.com/27001academy

Las acciones que las empresas pondrán en marcha como parte de los controles de Seguridad pueden materializarse a través de Normas, procedimientos, políticas, instructivos e incluso implantación de estrategias técnicas por ejemplo adquisición de software especializado o equipos con mayor performance. Por lo general, las organizaciones ya cuentan con la Infraestructura instalada en sus oficinas por ejemplo Firewall, Proxy, Data Center, etc., sin embargo, con lo que no se cuenta son con las reglas de manipulación o uso de las mismas en Beneficio de la Seguridad , es por ello que gran parte del tiempo de implementación de la Normas ISO 27001 estará reservada para la documentación .

De acuerdo a los expuesto anteriormente, la ISO 27001 nos proporciona un marco de trabajo minucioso de cómo unificar todos los elementos dentro del (SGSI).

La seguridad de Información no solo está limitada para temas de Tecnología, también engloba la gestión de la seguridad en los Procesos de Negocio, de las personas, de la Seguridad Física, Continuidad de las Operaciones y Temas Jurídicos etc.Podemos resumir la Seguridad de Información como la preservación de sus 3 Pilares:

1. **Confidencialidad.**

La información solo debe ser proporcionada a las personas autorizadas para el uso.

2. **Integridad.**

La información deberá ser exacta y sin alteraciones.

3. **Disponibilidad.**

La información deberá estar disponible cada vez que el usuario o proceso autorizado lo requiera

(SGSI Blog especializado en Sistemas de Gestión , 2018)

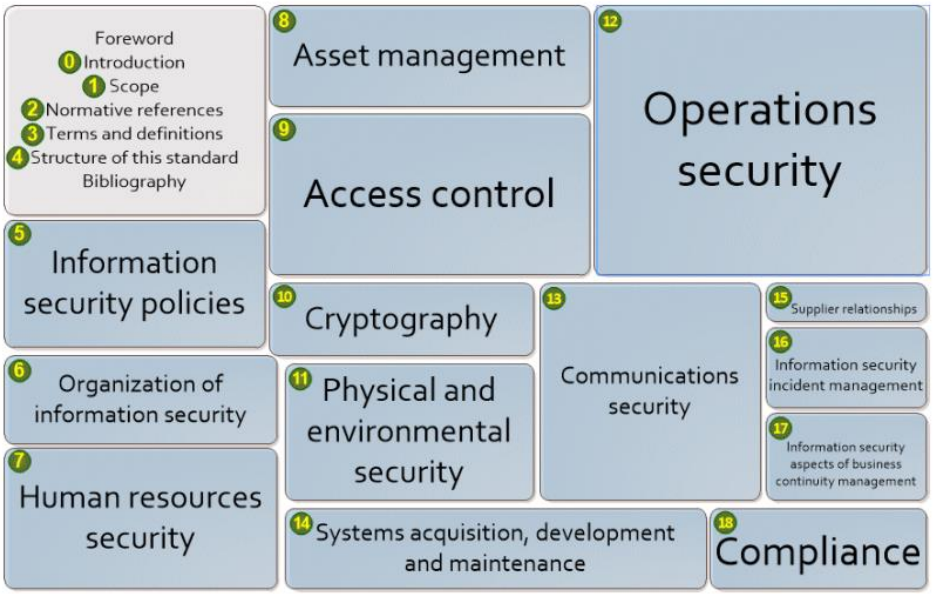
Figura N° 10 : Triada de Seguridad de Información

Fuente: Elaboración Propia

2.2.5.2. ISO/IEC 27002

Anexo de la Norma 27001**,** no es certificable para usuarios finales**.** Nos brinda una guía detallada para la implementación de los controles de seguridad señalados en la Norma ISO 27001. Actualmente se existen 114 controles, 35 Objetivos de Control que están distribuidos en 14 Dominios. En años anteriores se la conocía como **ISO/IEC 17799** y tiene sus inicios en la Norma Británica BS 7799-1. **(27001 Acdemy, 2018)**

Figura N° 11 : ISO 27002 - Dominios



Fuente : (NOTICEBORED, 2018)

Figura N° 12 : ISO27002 - Controles de Seguridad

Fuente: (ISO 2700.ES, 2012)

2.2.6. ITIL (INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY)

Traducido al español ITIL significa **Biblioteca de Infraestructura de Tecnologías de Información** y puede definirse como un conjunto de buenas prácticas, que han sido consensuadas en base a la experiencia y con resultados excelentes en las Organizaciones. Estas buenas prácticas son usadas para la gestión , desarrollo y operaciones sobre servicios de TI .

> **ITIL** describe un método ordenado que certifica la calidad de los servicios TI. Nos brinda una descripción exacta de los procesos más relevantes de una Organización de TI, incluye listas de revisión para procedimientos, tareas y responsabilidades que nos pueden ayudar como guías para adaptarnos a las necesidades específicas de cada organización. **(van Bon, y otros, 2008, p. 9)**

En décadas anteriores a mediados de los años noventa, ITIL paso de ser solo una teoría a consolidarse como un **framework** para las Organizaciones a nivel mundial.
Para poder comprender todo este marco de trabajo es necesario tener claro algunos temas, los cuales se conceptualizan a continuación:

Buena Práctica. – Podríamos definirlo como aquellos métodos que en la aplicación real han resultado ser efectivos, independientemente del sector, tamaño o naturaleza de la Organización a la cual sea aplicado.

> ITIL, se presenta como una Best Practices, esto hace referencia a un enfoque o metodología que ha confirmado en la práctica su eficacia o validez. Se puede afirmar que estas Buenas Practicas sirven como apoyo robusto a las organizaciones que necesiten optimizar sus servicios de TI Para ello es conveniente seleccionar un estándar general que sea posible para todos como COBIT ITIL, PRINCE2 ,CMMI, o ISO IEC/20000. **(van Bon, y otros, 2008, p. 15)**

2.3. MARCO CONCEPTUAL

2.3.1. Automatización

Según La Real Academia de las Ciencias Físicas y Exactas define el concepto de automática como el conjunto de procedimientos y métodos para el reemplazo del Agente humano denominado Operario en actividades mentales y físicas que han sido configuradas anticipadamente. A acorde a la definición original expuesta se puede definir el concepto de automatización como la aplicabilidad de la automática al control de los Procesos. **(Ponsa Asensio, 2006, p. 11)**

Podemos definir la automatización de Procesos de TI, como la capacidad de los sistemas Informáticos para realizar tareas que primariamente son ejecutadas por personas. Esta automatización adicionalmente lleva un control, corrige y permite visualizar el estado de los Workflows y tareas; también procesa reportes del proceso en su totalidad.

Un dato relevante de la automatización de procesos es el feedback, dado que, a través de ella, permitirá que el sistema evalué, compare y haga correctivos de forma inmediata; esta respuesta en base a las condiciones que fueron configuradas y sin intrusión de humanos.

También, la automatización de procesos nos permite realizar la programación de tareas para que se realicen en momentos determinados de tiempo; puede existir dependencias de procesos precedentes o de factores de desencadenantes. Esto admite la configuración de tareas con antelación. **(Mendoza Azury, 2017)**

Se define como la acción y efecto de Automatizar . **(Real Academia Española, 2018)**

2.3.2. Automatizar

Convertir ciertos movimientos en movimientos automáticos o indeliberados.
Aplicar la automática a un proceso o a un dispositivo. **(Real Academia Española, , 2018)**

En base a los autores consultados que fijan conceptos orientados hacia la automatización de procesos industriales y de procesos, puedo a continuación definir un concepto propio para la presente investigación:

Puedo definir **Automatizacion** de la siguiente forma:

Capacidad de configurar las tareas realizadas de forma manual por un actor humano dentro de un Proceso Definido y reemplazarlas para que sean ejecutadas de forma automatica a traves de modelos de programación.

2.3.3. Ventajas y Desvenjas de la Automatizacion

Ventajas

- Genera ventaja competitiva sobre sus principales competidores.
- Nos genera un ahorro de costos considerados Operativos e incrementa la productividad
- La automatizacion ayuda a la no interrupcion de los Procesos y de esta forma poder satisfacer la demanda del cliente interno o externo como tambien de los sistemas.
- Nos brinda mayor tiempo para ejecutar tareas de analisis y acelera la instalación de aplicaciones o ejecucion de trabajos operativos . .
- Elimina el error operativo humano que puede presentarse en la ejeucion de alguna tarea dentro del Proceso,con lo cual mejora la eficacia del mismo .

- Nos genera una mayor visibilidad del Workflow ,permitiendo la extraccion de reportes de los estados de los Procesos . .
- Puede implementarse en arquitectiras On Premise , como tambien en servicios Cloud . **(Mendoza Azury, 2017)**

Desventajas

- **Una de las principales desventajas , es el miedo de perder sus puestos de trabajo .** Es lógico pensar que un empelado al ver que sus tareas estan siemdo realizadas por un Robot o sistema informatico tenga el temor que en algun momento será despedido , muy por el contrario aquellas empresas que aplican la automatizacion al ser más eficientes generan mayores puestos de trabajo al tener mayor disponibilidad para ofrecer otros Servicios hacia los clientes.
- **Los Costos de inversión son muy elevados**. En muchos casos las Organizaciones suelen pensar que automatziar sus procesos es una inversion de miles de dolares y cuyo retorno de inversion es muy lento. Este punto puede ser evaluado dado que el costo Beneficio de implemantar una automatizacion en la Nube resulta menos costoso que el Proceso no automatizado implementado en la actualidad.
- **La flexibilidad del Proceso se pierde**. La organización puede suponer que con la automatizacion la modificacion de los Workflow resultaría un poco engorroso y poco flexibles . Sin embargo esto puede mitigarse siempre que se tenga el asesoramiento de la empresa que nos brindará el servicio , un buen analisis de lo que queremos para la empresa en el futuro nos ayudará a seleecionar un producto que tenga escalabilidad y evitaría estos problemas en el futuro. **(Mendoza Azury, 2017)**

2.3.4. Información

Su Estrecha relacion con los Datos y la toma de Decisiones

Es un Conjunto de datos vinculados que tienen un significado, de modo tal que minimizan la incertidumbre y amplían el conocimiento de quienes se avecinan a observarlos. Los datos se encuentran utilizables para su uso inmediato y sirven para aclarar las incertidumbres sobre temas determinados. **(Chiavenato Idalberto, 2006, p. 110)**

Consiste en un conjunto de datos que han sido clasificados y ordenados con un propósito determinado . **(Czinkota Michael, 2001, p. 115)**

La información registrada en Soportes o Medios

Existen muchas clases de información, pero el concepto más relevante es el que hace referencia a la información que se anuncia y se expresa a través de los Medios de Comunicación. **(López Yepez José, 2004)**

2.3.5. Tipos de Informacion

Información Científica: Este tipo de información considerada lógica es adquirida durante el proceso del conocimiento, muestra apropiadamente las leyes que rigen la realidad objetiva y es utilizada en la práctica de la Historia . **(Mijailov & Guilarirvkii, 1973)**

Información Bibliográfica: Se considera a toda Información de corte cientifico que se encuentra incluida en los documentos que pueden grabarse y leerse a traves de un

computador y considerada como entidad única, lógica ,completa e independiente. **(Martínez de Sousa, 2004)**

Información Documental: Es la Información incluida en los documentos , que pueden estar escritos (ejemplo bibliotecas, archivos o hemerotecas), en íconos (iconotecas, museos) o Sonoros (fonotecas ,discotecas). **(Martínez de Sousa, 2004, p. 516)**

Información Digital: La sustentada en la combinación numérica denominada digital y que tiene su expresión en texto, música e imagen **(López Yepez José, 2004, p. 59)**

2.3.6. Clasificación de Información

En cuanto a los criterios para su clasificación, tal como hemos comentado antes, vamos a basarnos en el carácter confidencial. ISO 27001 no plantea los niveles de clasificación a seguir, sino que da flexibilidad para que cada organización adopte aquel más empleado en función de la industria. Así, por ejemplo, para una organización de mediano tamaño, podríamos definir los siguientes 4 niveles para clasificar el carácter confidencial de su información:

Confidencial (cuando presenta un nivel mayor de confidencialidad).
Restringida (nivel medio de confidencialidad).
De uso interno (nivel más bajo de confidencialidad)
Público (cuando la información es accesible a todo el público)
(ISOTools, 2016)

2.4. MARCO METODOLOGICO

2.4.1. DISEÑO DE LA INVESTIGACION

Este proyecto de Investigación será desarrollado basándonos en el Diseño experimental de tipo **experimental**, pues es el que mejor se adapta a las necesidades del estudio.

El diseño experimental busca evaluar a través de probabilidades la dependencia que existe entre las variables definidas y con ello tener el sustento para poder reafirmar o refutar la hipótesis planteada y que fue sometida a pruebas.

2.4.2. ENFOQUE DE LA INVESTIGACION

En el Presente Proyecto de Investigación se busca demostrar la hipótesis, así como los objetivos planteados al inicio, el trabajo será desarrollado siguiendo las directrices del enfoque metodológico cuantitativo.

2.4.3. FUENTES DE INFORMACION

Para la presente investigación nuestra fuente de información será:

2.4.3.1. Secundaria:

Dado que se utilizará una BD Excel donde se encuentra consolidada la información histórica de los usuarios que han cesado en el Banco Financiero, en este archivo se encuentra registrada la Fecha de Cese y la fecha de ejecución de las bajas que son los campos necesarios para los cálculos de nuestro estudio.

2.4.3.2. Primaria:

En base al Archivo Histórico de Ceses se hará el cálculo del tiempo transcurrido desde la fecha de notificación del Cese hasta la Ejecución.

1. En base al Archivo Histórico de Ceses se hará el cálculo del esfuerzo en horas/hombre invertido por cada Cese.
2. Se construirá una matriz de riesgos en Base a la Metodología de Riesgos escogida.

2.3.4. POBLACION Y MUESTRA

2.3.4.1. POBLACIÓN

- ✓ Colaboradores Cesados del Banco Financiero del Perú Periodo enero 2017 – diciembre 2017
- ✓ Especialistas, usuarios Expertos del Comité de Seguridad de Información (30 Usuarios)

Criterios de Inclusión

1. Colaboradores de Sexo Femenino y Masculino.
2. Colaboradores pertenecientes a cualquiera de las Gerencias del Banco Financiero
3. Colaboradores que desempeñen cualquier cargo (Alta Rotación o Estándar)

Criterios de Exclusión

1. No se considera colaboradores pertenecientes a los Grupos de Negocio del Banco Financiero (Diners Club, Diners Travel, Crecer Seguros, Amerika Financiera, Amerika Brokers)
2. No se consideran colaboradores Tercerizados (Technology Outsourcing)
3. No se considera usuarios Cesados anteriores al año 2017.

2.3.4.2. MUESTRA

Se considera como **no Probabilística Muestreo por Criterio**, esto se sustenta a que el proceso de Cese del Banco Financiero fue estandarizado a partir del año 2014, sin embargo, la madurez del Proceso puede considerarse a partir del año 2017 (**Juicio de Experto – Especialista de Accesos**).

Es por eso que nuestra muestra para la investigación será la Base de Datos histórica de Ceses del periodo enero 2017 – Julio 2018.

Además, por el criterio técnico y conocimiento del negocio, la encuesta será segmentada solo a usuarios del Comité de Seguridad de Información.

2.3.5. TECNICA DE RECOLECCION

Por la naturaleza de la investigación cuyo objetivo es poder confirmar la hipótesis General que el diseño de la automatización del mantenimiento de Usuarios en el Proceso de Ceses del Banco Financiero reduce el riesgo de fuga de información, los datos necesarios serán recolectados de la siguiente forma:

1. Se utilizará la Base Histórica de Ceses del año enero 2017 – diciembre 2017, esta información se encuentra consolidada en un archivo Excel en el repositorio centralizado del área de Seguridad Informática – Control de Accesos. Para ello se cuenta con los permisos de Read y Write sobre el directorio.

2. El archivo de Ceses histórico será trabajado para poder calcular los tiempos de respuesta, esto corresponde a una fuente primaria que no existe actualmente:

   2.1 $F(n) = Fecha\ de\ Notificacion$

2.2 $F(e) = Fecha\ de\ Ejecucion$

2.3 $T(e) = Tiempo\ de\ Ejecucion$

3. En base a la metodología de riesgo seleccionada se calculará el riesgo de fuga de información que existe actualmente en el Banco Financiero $R(a) = Riesgo\ de\ Informacion\ Actual$

4. Diseño de la automatización de Mantenimiento de usuarios en el proceso de Ceses para el Banco Financiero.

5. Se entregará un cuestionario a cada miembro del Comité de Seguridad de Información para conocer la percepción actual del Mantenimiento de Usuarios en el Proceso de Ceses.

6. Luego del Diseño de la automatización el mantenimiento de usuarios para el Proceso de Ceses, se hará nuevamente el cálculo de los datos señalados en el punto 1 : $T(r) = Tiempo\ de\ Ejecucion$ y $R(a) = Riesgo\ de\ Informacion\ Actual$

7. Se entregará un cuestionario a cada miembro del Comité de Seguridad de Información para conocer la percepción del Mantenimiento de Usuarios en el Proceso de Ceses luego de conocer el nuevo Diseño.

CAPITULO 3

DESARROLLO DEL DISEÑO

Para el desarrollo de esta capitulo lo vamos a dividir en tres fases:

1) **Calculo de Valores Actuales Bajo el Proceso de Ceses Actual:** En esta primera fase nos centraremos en calcular los valores actuales de las variables que serán usadas para la confirmación de la Hipótesis en la presente investigación
2) **Desarrollo del Nuevo Diseño del Proceso de Ceses:** En esta fase vamos a diseñar el nuevo proceso de Mantenimiento de Usuarios orientado a la automatización de actividades que actualmente se realizan de forma manual.
3) **Simulación del Proceso Ceses Bajo nuevo Diseño:** Simulación del nuevo diseño del Proceso de Mantenimiento de Usuarios y evaluación de resultados.

3.1. CALCULO DE VALORES ACTUALES BAJO EL PROCESO DE CESES ACTUAL

.

CALCULO TIEMPO DE EJECUCION:

Para calcular este valor, vamos a utilizar la Base de Datos Histórica de Ceses correspondiente al periodo Enero 2017 – Diciembre 2017. Este archivo contiene los siguientes campos:

Tabla N° 1 : Información De Usuarios Cesados Bitácora Actual

CÓDIGO EMPLEADO	NOMBRE COMPLETO	CARGO	FECHA DE CESE	FECHA NOTIFICACIÓN DE CESE	FECHA EJECUCIÓN	**TIEMPO DE EJECUCIÓN**
6173	Joel Acosta	ANALISTA DE SEGURIDAD	31/10/2015	31/10/2015	02/11/2015	Valor Calculado

Fuente: Elaboración Propia

(*) Por temas de confidencialidad en la presente investigación solo trabajaremos con los campos de la muestran que serán útiles para las mediciones. La información personal será suprimida.

$F(n) =$ Fecha de Notificación de Cese (**Formato Fecha** dd/mm/aa)

$F(e) =$ Fecha de Ejecución de Cese (**Formato Fecha** dd/mm/aa)

$T(e) =$ Tiempo de Ejecución de Cese = $F(e) - F(n)$
(Este valor será expresado en Horas)

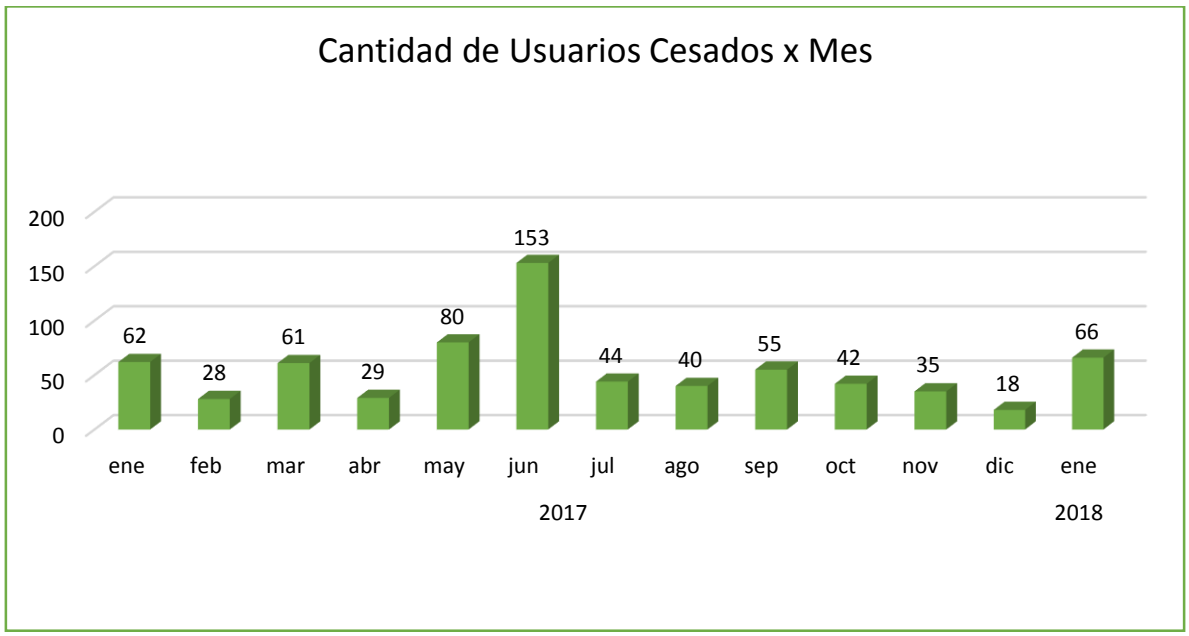
Antes de empezar a realizar los cálculos procedemos a normalizar la Base de Datos Excel. A continuación, mostraremos los Tiempos de Ejecución promedio mensual:

Tabla N° 2 : Cantidad de Usuarios Cesados por Mes

Periodo	Cantidad de Ceses
2017	
ene	62
feb	28
mar	61
abr	29
may	80
jun	153
jul	44
ago	40
sep	55
oct	42
nov	35
dic	18
Total general	**647**

Fuente: Elaboración Propia

Figura N° 13 : Cantidad de Usuarios Cesados Mensual



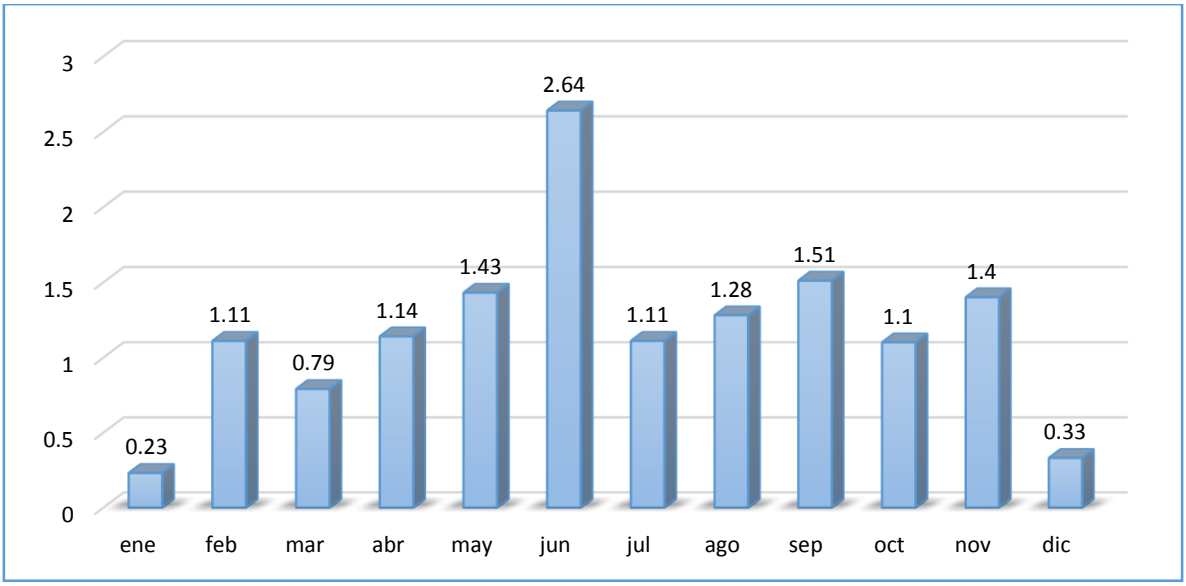
Fuente: Elaboración Propia

Tabla N° 3 : Tiempo de Ejecución Promedio de Ceses Mensual

Periodo	Tiempo Promedio Ejecución (días)
2017	
ene	0.23
feb	1.11
mar	0.79
abr	1.14
may	1.43
jun	2.64
jul	1.11
ago	1.28
sep	1.51
oct	1.10
nov	1.4
dic	0.33
Total general	**1.17**

Fuente: Elaboración Propia

Figura N° 14 : Promedio Tiempo Ejecución Cese Mensual



Fuente: Elaboración Propia

CALCULO DE CARGA OPERATIVA

Actualmente el equipo de Control de Accesos administra 56 aplicaciones del Banco Financiero y se tiene 637 perfiles definidos dentro del maestro de Perfilamiento (Anexo N° 1 Referencial).

Para poder calcular la carga Operativa diaria equivalente en Horas Hombres que representa la atención de este servicio, seguiremos los siguientes pasos

1. El cálculo del esfuerzo en horas/hombre solo será aplicado a los 4 sistemas críticos definidas por el Negocio (**Red, Correo Corporativo, Microfinanzas, IBS**) y a la actividad de Baja en el sistema. En la siguiente tabla podemos observar la descripción breve del sistema y la actividad:

Tabla N° 4 : Aplicaciones Críticas del Banco Financiero

Sistema	Descripción
APLICACIONES	
RED	Son las cuentas de usuarios creadas en el directorio Activo para que puedan autenticarse a la red Interna del Banco Financiero y poder utilizar los recursos .
CORREO	Servicio de mensajería que actualmente está implementado en un entorno Hibrido Exchange On Premise y Cloud Plataforma Office 365 –Exchange Online .
IBS	Core del Negocio en donde se registran las operaciones transaccionales del Banco, implementado en AS400 .
MICROFINANZAS	Sistema desarrollado en Visual Basic y utilizado para el registro, aprobación y desembolso de créditos al sector MYPE.
TAREAS ASOCIADAS AL PROCESO DE CESE	
CA SERVICE DESK	Herramienta de Gestión de Requerimientos e Incidentes generados por usuarios internos del Banco Financiero. ,
GRP	Grupo de Distribución de Correo , utilizado para el envío de notificaciones de forma masiva ,
BD CESES	Archivo en Excel utilizado internamente para el registro y seguimiento de los Ceses de Usuario.

Fuente: Elaboración Propia

Tabla N° 5 : Tiempo Promedio de Ejecución de Cese de las Aplicaciones

Sistema	Actividad en el Sistema	Esfuerzo Minutos
RED	Baja de Usuario	3
CORREO	Baja de Usuario	3
IBS	Baja de Usuario	3
MICROFINANZAS	Baja de Usuario	5
CA SERVICE DESK	Registro deTicket	5
GRP	Notificación d involucrados del Proceso	3
BD CESES	Registro de usuarios Cesados	3
TOTAL MINUTOS		**25 minutos**
TOTAL HORAS		**0.42 horas**

Fuente: Elaboración Propia

Un Cese de usuario representa 25 Minutos y en equivalencia en horas tenemos:

$$\boldsymbol{Tiempo\ en\ Horas} = \frac{\text{Tiempo en Minutos}}{60}$$

$$\boldsymbol{Tiempo\ en\ Horas} = \frac{25}{60}$$

$$\boldsymbol{Tiempo\ en\ Horas} = \mathbf{0.42}$$

(*) Importante. - El cálculo ha sido recabado en base a la operativa del usuario experto del equipo de Seguridad TI – Control de Accesos.

Hemos calculado que **1 Cese de Usuario** representa **0.42 horas/hombre en promedio x día.**

Como siguiente paso vamos a calcular el promedio de usuarios Cesados por día. Para ello haremos un nuevo cálculo, utilizando la información de la **Tabla N° 2 .**

Consideraciones;

1. Solo se considerará para el cálculo días Laborales, quiere decir que son 4 semanas efectivas que equivalen a 20 días.

Tabla N° 6 : Promedio de Ceses Mensual

Periodo	Cantidad de Ceses x Mes
2017	
ene	62
feb	28
mar	61
abr	29
may	80
jun	153
jul	44
ago	40
sep	55
oct	42
nov	35
dic	18
ene	66
Promedio de Ceses Mensual	**53.92**

Fuente: Elaboración Propia

$$\text{Promedio de Cese Diario} = \frac{\textbf{Promedio de Cese Mensual}}{\textbf{20}}$$

$$\text{Promedio de Cese Diario} = \frac{53.92}{20}$$

$$\text{Promedio de Cese Diario} = 2.7$$

Entonces haciendo un resumen tenemos la siguiente información:

1. Cantidad Promedio de Ceses Diarios: **2.7 Usuarios**
2. Tiempo Promedio de Ejecución de Cese Diario: **0.42 Horas**

$$\textbf{Carga Operativa} = \text{Cantidad Promecio Ceses x Tiempo Promedio Ceses}$$

$$\textbf{Carga Operativa Diaria} = 2.7 * 0.42$$

$$\textbf{Carga Operativa Diaria} = 1.13\ \text{Horas}/Hombre$$

CALCULO DE ERRORES MANUALES

Esta información es considerada como fuente primaria dado que será tomada de las observaciones de Auditoria Interna Anual a los cuales hemos sometidos en el año 2017, para tal efecto tomaremos como referencia las observaciones encontradas sobre las 4 aplicaciones críticas; Red, IBS, Microfinanzas y Correo Electrónico.

En base al principio de Confidencialidad, la información presentada omitirá cualquier dato de índole personal y solo servirá como referencia para los cálculos. El cálculo de errores manuales será representado como el Porcentaje de usuarios que no fueron cesados sobre la cantidad de User con acceso correspondiente al perfil.

$$\%\ \boldsymbol{Errores\ Manuales} = \frac{\text{Cantidad de Usuarios con accesos a la aplicacion no Cesados}}{\text{Cantidad de Usuarios con accesos a la aplicacion}}$$

$$\%\ \boldsymbol{Efectividad} = 1 - \ \%\ Errores\ Manuales$$

Muestra Enero 2017 – Diciembre 2017

$$\boldsymbol{Total\ Usuarios\ Cesados} = 647$$

Red - Errores Manuales

Observación Auditoria: Usuarios Cesados Activos = 38

Cantidad de Usuarios con accesos a la aplicacion no Cesados $= 38$

Cantidad de Usuarios con accesos a la aplicacion; 647

$$\% \boldsymbol{Errores\ Manuales} = \frac{38}{647}$$

$$\% \boldsymbol{Errores\ Manuales} = 0.05 = 5\ \%$$

$$\% \boldsymbol{Efectividad} = 1 - \ \% Errores\ Manuales$$

$$\% \boldsymbol{Efectividad} = 1 - \ 0.05 = 0.95 = 95\ \%$$

Correo Electrónico - Errores Manuales

Observación Auditoria: Usuarios Cesados Activos = 38

Cantidad de Usuarios con accesos a la aplicacion no Cesados $= 38$

Cantidad de Usuarios con accesos a la aplicacion; 647

$$\% \boldsymbol{Errores\ Manuales} = \frac{38}{647}$$

$$\% \boldsymbol{Errores\ Manuales} = 0.05 = 5\ \%$$

$$\% \boldsymbol{Efectividad} = 1 - \ \% Errores\ Manuales$$

$$\% \boldsymbol{Efectividad} = 1 - \ 0.05 = 0.95 = 95\ \%$$

IBS - Errores Manuales

Observación Auditoria: Usuarios Cesados Activos = 11

Cantidad de Usuarios con accesos a la aplicacion no Cesados $= 11$

Cantidad de Usuarios con accesos a la aplicacion; 647

$$\% \boldsymbol{Errores\ Manuales} = \frac{11}{647}$$

$$\% \boldsymbol{Errores\ Manuales} = 0.02 = 2\ \%$$

$$\% \boldsymbol{Efectividad} = 1 - \ \% Errores\ Manuales$$

$$\% \boldsymbol{Efectividad} = 1 - \ 0.02 = 0.98 = 98\ \%$$

Microfinanzas - Errores Manuales

Observación Auditoria: Usuarios Cesados Activos = 8

Cantidad de Usuarios con accesos a la aplicacion no Cesados $= 8$

Cantidad de Usuarios con accesos a la aplicacion; 186

$$\% \boldsymbol{Errores\ Manuales} = \frac{8}{186}$$

$$\% \boldsymbol{Errores\ Manuales} = 0.04 = 4\ \%$$

$$\% \boldsymbol{Efectividad} = 1 - \ \% Errores\ Manuales$$

$$\% \boldsymbol{Efectividad} = 1 - \ 0.4 = 0.96 = 96\ \%$$

CALCULO DE RIESGO DE FUGA DE INFORMACION

Tenemos clara la definición del Riesgo:

$$\boldsymbol{Riesgo} = \text{Probabilidad de Ocurriencia} * \text{Impacto}$$

A continuación, definiremos algunos conceptos:

Vulnerabilidad: Debilidad que esta inherente en un Activo de Información.

Amenaza: Explota las vulnerabilidades.

Riesgo: Efecto de la Incertidumbre en la consecución de los Objetivos de la Empresa.

Para el presente estudio tenemos las siguientes variables:

Vulnerabilidad: Cuenta de Usuarios Cesados que permanecen activas en aplicaciones.

Amenaza: Ex Colaboradores sin Ética Profesional.

Riesgo: Fuga y Perdida de Información

Para poder hacer una Gestión de Riesgos alineada a los objetivos estratégicos de la Organización es necesario poder seguir una metodología, que consiste en una serie de pasos lógicos y ordenados que puede verse gráficamente a continuación:

Figura N° 15 : Esquema de la Gestión de Riesgos

Fuente: Elaboración Propia

1. DEFINICION DEL CONTEXTO:

En este punto vamos a identificar el contexto en el cual se está desenvolviendo actualmente el Banco Financiero.

Se ha identificado 5 sectores principales que tienen influencia directa sobre la orgenciazión:

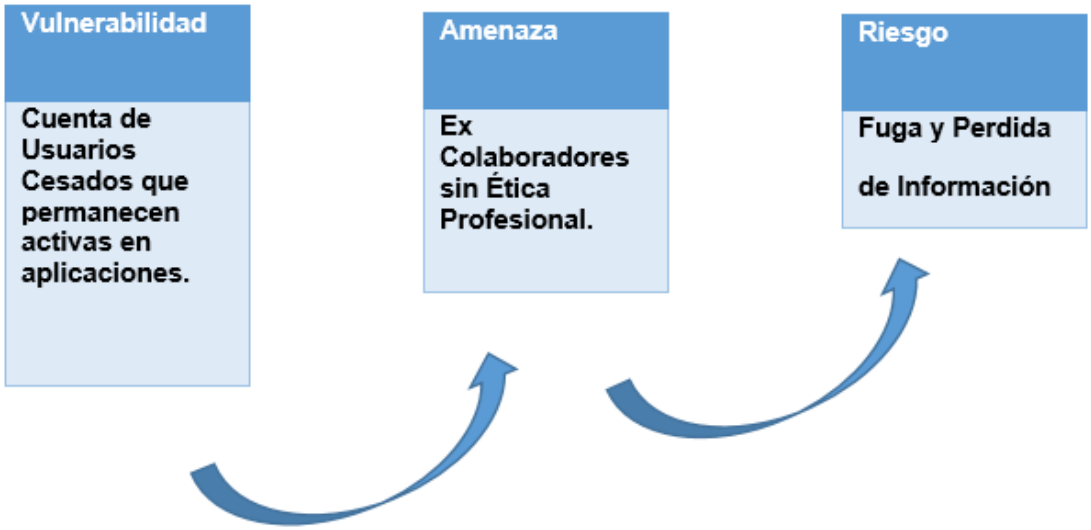
Figura N° 16 : Contexto Banco Financiero

Fuente: Elaboración Propia

2. IDENTIFICACION DEL RIESGO

En Base al contexto interno y externo descrito anteriormente, podremos identificar los riesgos potenciales que podrían afectar a nuestra organización. Para el presente estudio:

Figura N° 17 : Identificación del Riesgo en el Proceso de Ceses



Fuente: Elaboración Propia

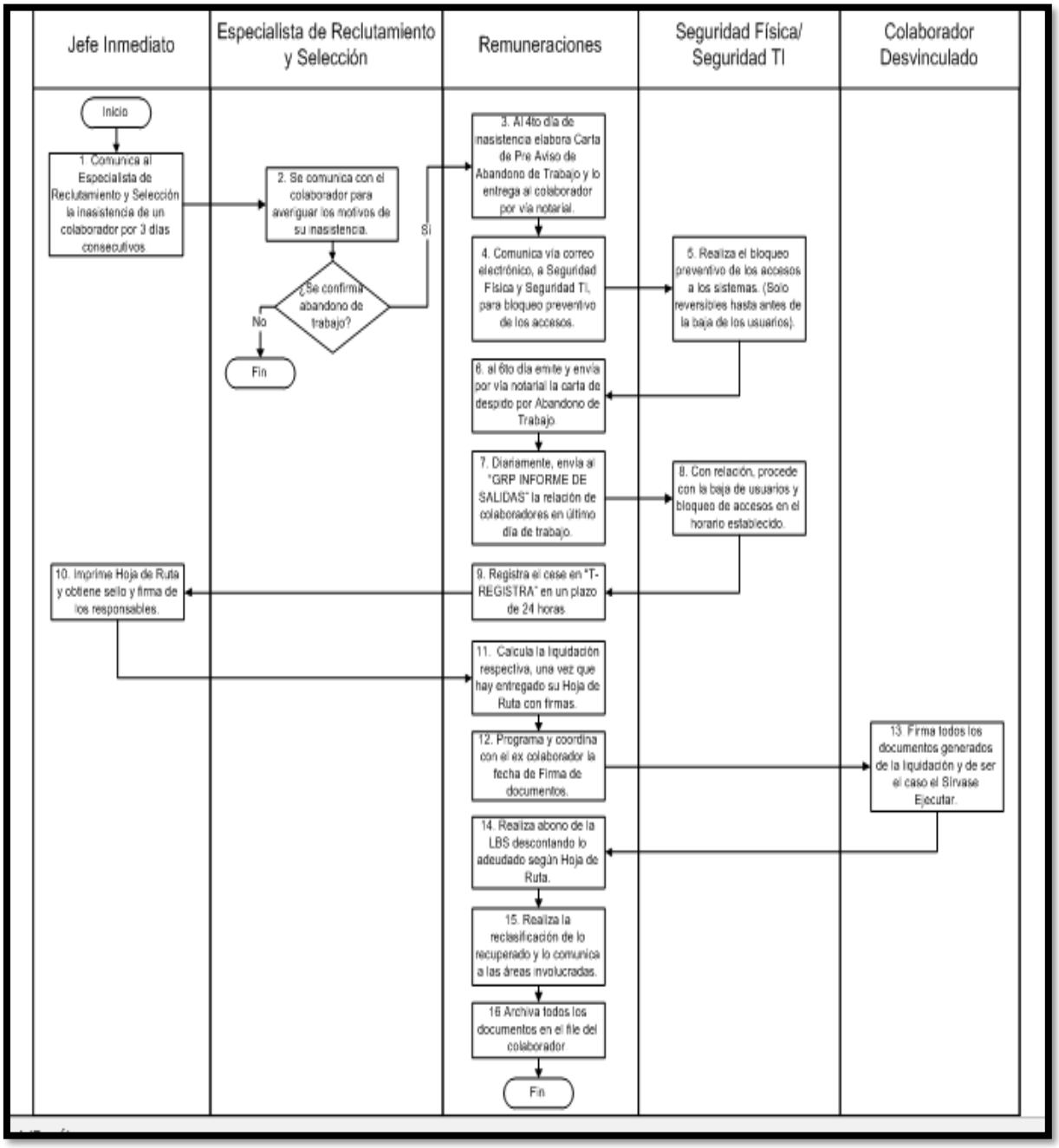
Para Identificar el riesgo descrito nos estamos basando en 3 herramientas:

1. **Juicio de Experto. –** Consideramos este elemento a aquellas personas que son parte activa del Proceso de Ceses para el Banco Financiero ‘’Especialista de Control de Accesos de Tata y Especialistas de Seguridad de Información Banco Financiero’’, quien desde su perspectiva y experticia podrá proporcionarnos valores para los cálculos.

2. Proceso Documentado Actual. –

En el siguiente flujograma podremos observar todas las interrelaciones que existen en el Proceso de Ceses de Usuarios del Banco Financiero del Perú

Figura N° 18 : Flujograma Completo del Proceso de Cese de Usuarios



Fuente: Portal de Normas del Banco Financiero del Perú

En la siguiente figura podemos visualizar las actividades del Proceso de Ceses que interrelacionan los equipos de **Gestión de Personas** quienes notifican el Cese y **Seguridad TI** quienes ejecutan el mismo.

Figura N° 19 : Flujograma de Proceso Cese Gestión de Personas – Seguridad TI

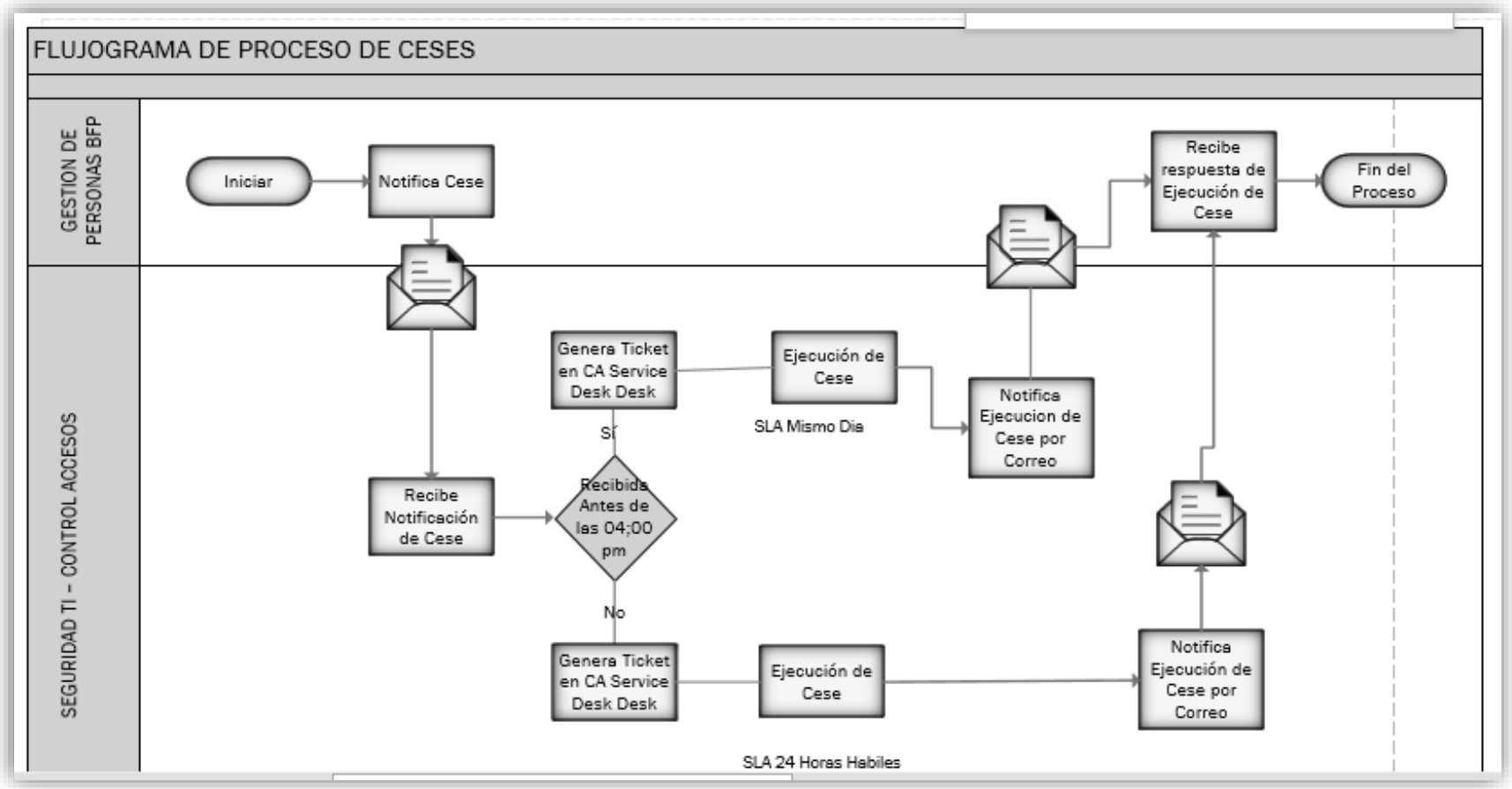


Diagrama de Actividades

A continuación, se detalla la secuencia de actividades del Proceso de Cese de Usuarios del Banco Financiero.

Tabla N° 7 : Diagrama de Actividades del Proceso de Ceses

Responsable	N° Operación	Descripción	Registros / Evidencias
GP (Unidad Remuneraciones)	1	Gestión de Personas del Banco Financiero notifica el Cese de Colaborador por correo electrónico al GRP SALIDAS.	Alarma con datos del colaborador
Seguridad TI	2	Revisa la información recibida.	
	3	¿La notificación llego antes de las 04;00 pm? SI: Continúa Paso 4. NO: Continúa Paso 7	
	4	Se genera el Requerimiento en la herramienta de Gestión CA Service Desk	Ticket Registrado
	5	Ejecuta Baja de Usuario en las aplicaciones Críticas el mismo día .	
	6	Notifica por correo electrónico la ejecución del Cese al GRP SALIDAS..	Correo Electrónico de Confirmación
	7	Se genera el Requerimiento en la herramienta de Gestión CA Service Desk	Ticket Registrado
	8	Ejecuta Baja de Usuario en las aplicaciones Críticas el mismo día .	
	9	Notifica por correo electrónico la ejecución del Cese al GRP SALIDAS..	Correo Electrónico de Confirmación
GP (Unidad Remuneraciones	10	Recibe confirmación de Cese	

Fuente : Elaboración Propia

En Base a la información analizada podemos plantear las siguientes interrogantes con sus respectivas respuestas:

A: ¿Qué es lo que puede suceder?

Fuga o Pérdida de Información crítica del Banco Financiero., que puede ser distribuida de forma indiscriminada a través de canales informales a personas u empresas de la competencia.

B: ¿Cómo y porque puede suceder?

Al existir una brecha de tiempo entre la Fecha de notificación del Cese y la ejecución del mismo, las cuentas de usuario de las aplicaciones permanecen activas a pesar que la notificación de Cese ya fue remitida a Control de Accesos.

Escenarios:

- Fines de Semana
- Feriados Calendario
- Capacidad del Servicio Desbordada
- Feriado por Cumbres o Eventos Nacionales no calendarizados.

C: Clasificar el Riesgo

En este presente estudio podemos clasificar al riesgo asociado como un ***''Riesgo Operativo"*** dado que existen deficiencias en el Proceso Actual tanto manual y carencia de herramientas Tecnológicas que automaticen la carga operativa.

D: Determinación de las Consecuencias

En este punto vamos a señalar el impacto que causaría la materialización del riesgo en nuestra Organización:

1. Pérdida de Confianza y Credibilidad de nuestros Clientes Actuales.
2. Disminución en la captación de nuevos Clientes.
3. Pérdida de reputación en el mercado.
4. Ventaja Competitiva de otros Bancos.
5. Demandas Legales por divulgación de Información crítica.
6. Plagio de nuevos Proyectos o Productos Financieros.
7. No renovación de Certificaciones Internacionales: PCI,27001, ASA etc.

3. ANALISIS DEL RIESGO

Para analizar el Riesgo estaremos usando la metodología implementada por el Banco Financiero alineada a (**Governance, Risk and Compliance**) donde se desarrolla Gobierno Corporativo, Administración de Riesgos y Cumplimiento Regulatorio

Para ello debemos tener claro los siguientes Conceptos:

- **Evento:** Se define como un suceso o serie de sucesos que pueden ser internos o externos a la Organización, ocasionados por la misma causa y que suceden durante el mismo periodo de tiempo**.** (Superintencia de Banca, 2009, p. 1)

- **Evento de seguridad de la información**: Se trata de una ocurrencia reconocida del estado de un sistema, servicio o red mostrando una potencial falla en la política de seguridad de la información o falla en los controles implementados, o una situación previamente indocumentada que puede ser relevante para la seguridad. (Superintencia de Banca, 2009, p. 2)

- **Probabilidad (P):** Está asociada a la frecuencia real o estimada de ocurrencia del riesgo, si no se aplica el control al activo de información.

- **Relevancia (Re)**: Nivel de importancia del activo para el negocio de la organización.

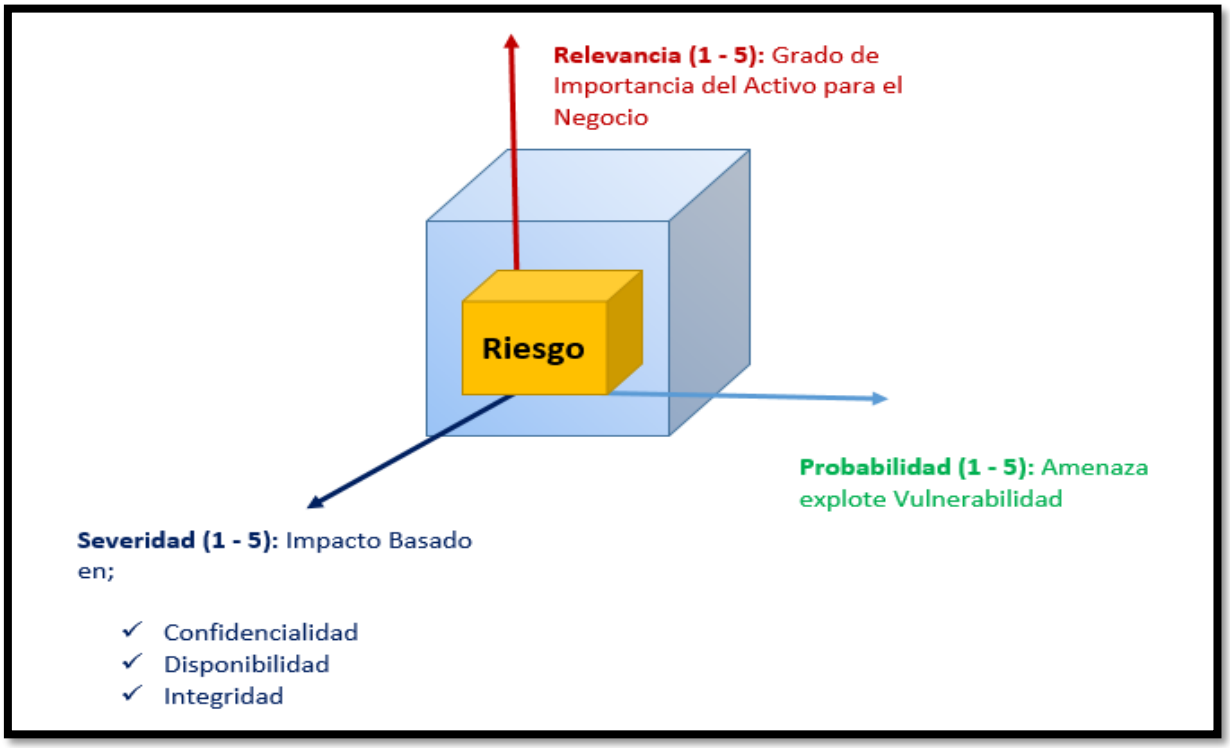
- **Riesgo (R)**: Es la probabilidad de que un evento ocurra debido a la ausencia de uno o varios controles de los activos de información, impactando en la organización.

- **Severidad (S):** Es la magnitud del impacto que puede causar el evento al activo de información, si se materializa el riesgo.

Método de Valoración de Riesgos

El método de valorización del Riesgo que será usado para esta investigación, se basa en la **Probabilidad (P), Severidad (S)** y **Relevancia (R)** y que están asociados a la ausencia de un control en los activos de información. En el siguiente gráfico podremos observar gráficamente nuestro marco metodológico de la valorización de riesgos.

Figura N° 20 : Valorización del Riesgo



Fuente: Elaboración Propia

Tabla N° 8 : Escala de Calificación de Probabilidad

Valor	Frecuencia	Descripción
1	Despreciable	1 Vez al Año
2	Muy Poco Frecuente	2 Veces al Año
3	Poco Frecuente	3 veces al año
4	Frecuente	4 – 5 Veces al año
5	Muy Frecuente	6 a más Veces al año

Fuente: Elaboración Propia

Tabla N° 9 : Escala de Calificación de Relevancia

Valor	Criterio		
	Confidencialidad	**Integridad**	**Disponibilidad**
	De exponerse el activo de información al acceso y/o divulgación de su contenido no autorizado a individuos, sistemas informáticos, entidades o procesos, éste:	De exponerse el activo de información a alguna alteración, degradación o corrupción de su exactitud, contenido, competencia (en caso de activos de tipo persona), de manera total o parcial, éste:	De exponerse el activo de información a su no acceso o no disponibilidad a las personas, entidades, procesos y demás entes autorizados, éste:
5 Muy Alto	Tendría un impacto muy alto o muy grave en la Organización.	Tendría un impacto muy alto o muy grave en la Organización.	Tendría un impacto muy alto o muy grave en la Organización.
4 Alto	Tendría un impacto alto o grave en la Organización.	Tendría un impacto alto o grave en la Organización.	Tendría un impacto alto o grave en la Organización.
3 Medio	Tendría un impacto medio en la Organización.	Tendría un impacto medio en la Organización.	Tendría un impacto medio en la Organización.
2 Bajo	Éste tendría un impacto bajo en la Organización.	Tendría un impacto bajo en la Organización.	Tendría un impacto bajo en la Organización.
1 Muy Bajo	Tendría un impacto muy bajo o insignificante en la Organización.	Tendría un impacto muy bajo o insignificante en la Organización.	Tendría un impacto muy bajo o insignificante en la Organización.

El valor de la relevancia total del activo evaluado será el promedio de la suma de Confidencialidad + Integridad + Disponibilidad:

$$Valor\ \ Relevancia\ del\ Activo = \frac{\text{Confidencialidad} + \text{Integridad} + \text{disponibilidadn}}{3}$$

Tabla N° 10: Escala de calificación de Impacto

Valor	Criterios de Supuestos Impactos para la Valoración de Activos				
	Información De Carácter Personal	**Obligaciones Legales**	**Seguridad**	**Intereses Comerciales o Económicos**	**Pérdida de Confianza (Reputación)**
5 Muy Alto	–Probablemente afecte gravemente a un grupo de individuos. –Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.	–Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación.	–Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.	–De enorme interés para la competencia. –De muy elevado valor comercial. –Causa de pérdidas económicas excepcionalmente elevadas –Causa de muy significativas ganancias o ventajas para individuos u organizaciones	–Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones –Probablemente causaría una publicidad negativa generalizada por afectar de forma

Valor	Criterios de Supuestos Impactos para la Valoración de Activos				
	Información De Carácter Personal	Obligaciones Legales	Seguridad	Intereses Comerciales o Económicos	Pérdida de Confianza (Reputación)
				– Constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros.	excepcionalmente grave a las relaciones a las relaciones con el público en general
4 Alto	– Probablemente afecte gravemente a un individuo. – Probablemente quebrante seriamente leyes o regulaciones.	– Probablemente cause un incumplimiento grave de una ley o regulación.	– Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.	– De alto interés para la competencia. – De elevado valor comercial – causa de graves pérdidas económicas. – Proporciona ganancias o ventajas desmedidas a individuos u	– Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones. – Probablemente causaría una publicidad negativa generalizada por

Valor	Criterios de Supuestos Impactos para la Valoración de Activos				
	Información De Carácter Personal	Obligaciones Legales	Seguridad	Intereses Comerciales o Económicos	Pérdida de Confianza (Reputación)
				organizaciones. – Constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros.	afectar gravemente a las relaciones con el público en general.
3 **Medio**	– Probablemente afecte a un grupo de individuos. – Probablemente quebrante leyes o regulaciones.	– Probablemente sea causa de incumplimiento de una ley o regulación.	– Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.	– De cierto interés para la competencia. – De cierto valor comercial. – Causa de pérdidas financieras o merma de ingresos. – facilita ventajas desproporcionadas a individuos u organizaciones. – constituye un incumplimi	– Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones. – Probablemente sea causa una cierta publicidad negativa por afectar negativamente a

Valor	Criterios de Supuestos Impactos para la Valoración de Activos				
	Información De Carácter Personal	Obligaciones Legales	Seguridad	Intereses Comerciales o Económicos	Pérdida de Confianza (Reputación)
				ento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros.	las relaciones con el público.
2 Bajo	– Probablemente afecte a un individuo. – Probablemente suponga el incumplimiento de una ley o regulación.	– Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación.	– Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente.	– De bajo interés para la competencia. – De bajo valor comercial.	– Probablemente afecte negativamente a las relaciones internas de la Organización. – Probablemente cause una pérdida menor de la confianza dentro de la Organización.

Valor	Criterios de Supuestos Impactos para la Valoración de Activos				
	Información De Carácter Personal	Obligaciones Legales	Seguridad	Intereses Comerciales o Económicos	Pérdida de Confianza (Reputación)
1 Muy Bajo	– Pudiera causar molestias a un individuo. – Pudiera quebrantar de forma leve leyes o regulaciones	– Pudiera causar el incumplimiento leve o técnico de una ley o regulación.	– Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente.	– De pequeño interés para la competencia. – De pequeño valor comercial. – Supondría pérdidas económicas mínimas.	– Pudiera causar una pérdida menor de la confianza dentro de la Organización. – No supondría daño a la reputación o buena imagen de las personas u organizaciones.

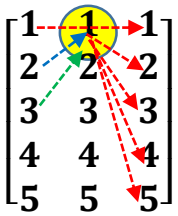
Fuente: Elaboración Propia

$$Valor\ \ Impacto$$

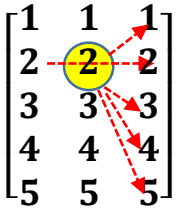
$$= \frac{Información\ de\ Carácter\ Personal + Obligaciones\ Legales + Seguridad + Intereses\ Economicos + Perdida\ de\ Confianza}{5}$$

Realizando la multiplicación respectiva para el cálculo de los **valores máximos y mínimos** del Nivel de Riesgo:

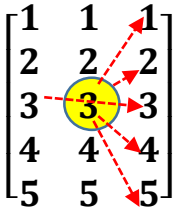
$$A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \\ 4 & 4 & 4 \\ 5 & 5 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 6 & 8 & 10 \\ 3 & 6 & 9 & 12 & 15 \\ 4 & 8 & 12 & 16 & 20 \\ 5 & 10 & 15 & 20 & 25 \end{bmatrix}$$



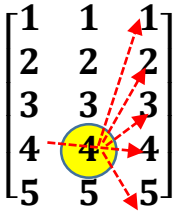
$$A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \\ 4 & 4 & 4 \\ 5 & 5 & 5 \end{bmatrix} = \begin{bmatrix} 2 & 4 & 6 & 8 & 10 \\ 4 & 8 & 12 & 16 & 20 \\ 6 & 12 & 18 & 24 & 30 \\ 8 & 16 & 24 & 32 & 40 \\ 10 & 20 & 30 & 40 & 50 \end{bmatrix}$$



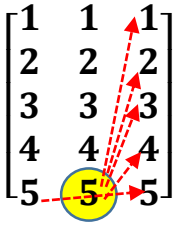
$$A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \\ 4 & 4 & 4 \\ 5 & 5 & 5 \end{bmatrix} = \begin{bmatrix} 3 & 6 & 9 & 12 & 15 \\ 6 & 12 & 18 & 24 & 30 \\ 9 & 18 & 27 & 36 & 45 \\ 12 & 24 & 36 & 48 & 60 \\ 15 & 30 & 45 & 60 & 75 \end{bmatrix}$$



$$A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \\ 4 & 4 & 4 \\ 5 & 5 & 5 \end{bmatrix} = \begin{bmatrix} 4 & 8 & 12 & 16 & 20 \\ 8 & 16 & 24 & 32 & 40 \\ 12 & 24 & 36 & 48 & 60 \\ 16 & 32 & 48 & 64 & 80 \\ 20 & 40 & 60 & 80 & 100 \end{bmatrix}$$



$$A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \\ 4 & 4 & 4 \\ 5 & 5 & 5 \end{bmatrix} = \begin{bmatrix} 5 & 10 & 15 & 20 & 25 \\ 10 & 20 & 30 & 40 & 50 \\ 15 & 30 & 45 & 60 & 75 \\ 20 & 40 & 60 & 80 & 100 \\ 25 & 50 & 75 & 100 & 125 \end{bmatrix}$$



Ordenando los Valores Obtenidos, tenemos el siguiente resumen:

Tabla N° 10 : Valores de Riesgo Calculados

Valores Posibles PSR					
1	2	3	4	5	6
8	9	10	12	15	16
18	20	24	25	27	30
32	36	40	45	48	50
60	64	75	80	100	125

Fuente: Elaboración Propia

El valor de riesgo **PSR** representa el grado de riesgo asociado a la ausencia de un control de Seguridad . El resultado es un valor numérico entero dentro del intervalo 1 y 125, con su respectivo nivel variando conforme al resultado de la multiplicación. Las acciones a tomar de acuerdo al Nivel de Riesgo calculado serán de la siguiente forma:

Tabla N° 11 : Acciones a Tomar Según Nivel de Riesgo

ACEPTAR	**MITIGAR**
No se realizan acciones de mitigación ni control sobre el mismo; asumiendo el nivel de probabilidad e impacto del riesgo.	Se establece, planifica y ejecuta medidas (planes de acción), dirigidas a reducir o disminuir el nivel de probabilidad de ocurrencia y/o de impacto del riesgo. Establecer un plan de acción, comprende definir el alcance para tratar los principales riesgos residuales identificados, así como el responsable de diseñar e implementar el plan de acción y establecer el plazo para ello.
EVITAR	**TRANSFERIR**
Eliminar o rediseñar las actividades o procesos, que dan origen a situaciones de riesgo.	Se transfiere a un tercero (Proveedor/ Seguro), la obligación por las consecuencias que puede originar el riesgo.

Fuente: Elaboración Propia

Tabla N° 12 : Nivel de Riesgo

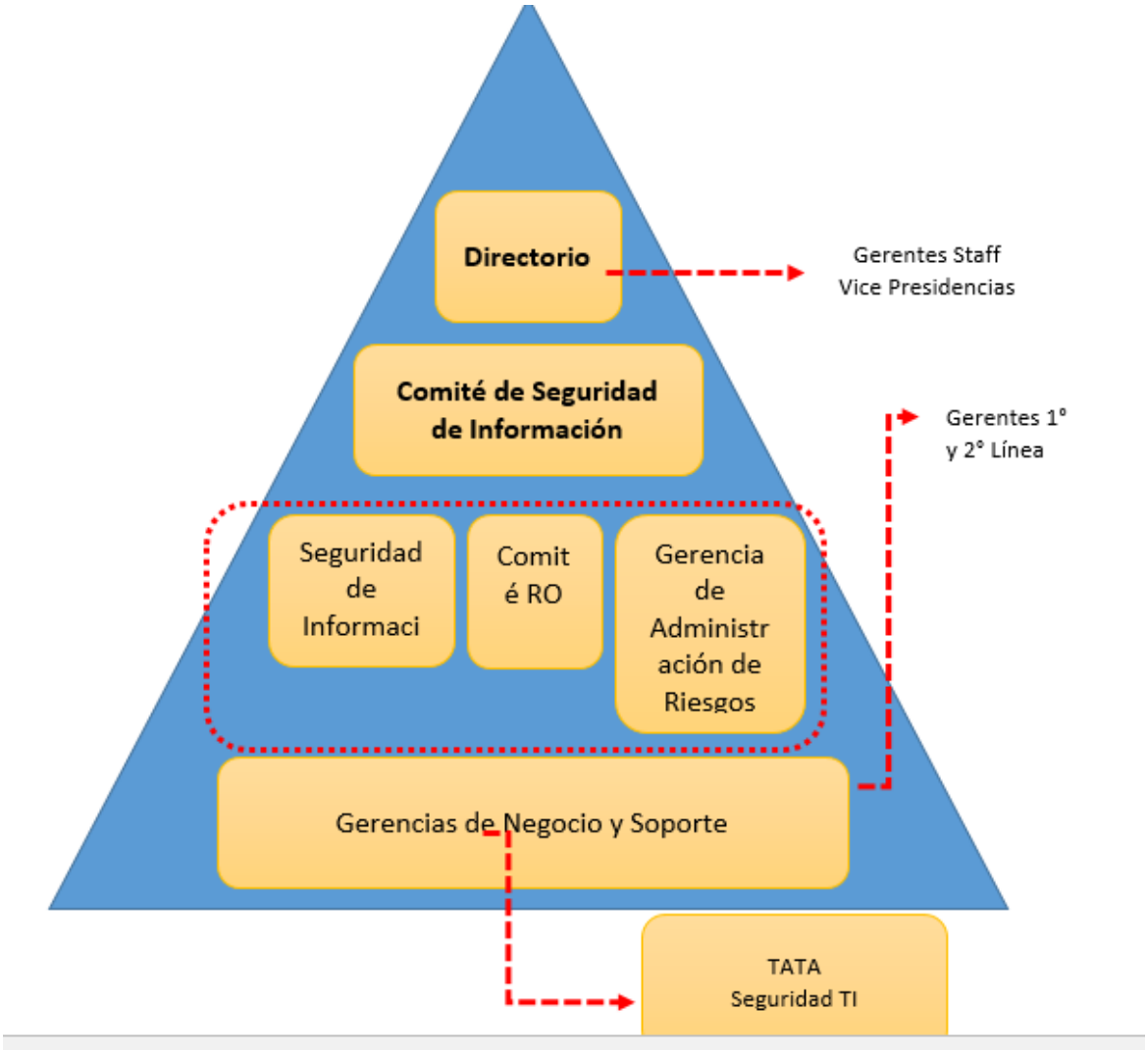
Nivel de Riesgo de Control PSR		Acciones a Tomar
Nivel de Riesgo	Rango de Valores P*S*R	
Muy Bajo	1, 2, 3, 4, 5, 6	Son riesgos aceptables y deben ser informados para los Propietarios de los activos
Bajo	8, 9, 10, 12, 15, 16	Son riesgos que pueden ser aceptables después de revisión y confirmación de los Propietarios de los activos.
Medio	18, 20, 24, 25, 27, 30	Son riesgos que pueden ser aceptables después de la revisión y confirmación de los Propietarios de los activos, todavía la aceptación del riesgo debe ser hecha por medios formales.
Alto	32, 36, 40, 45, 48, 50	Son riesgos inaceptables y los Propietarios de los activos deben ser orientados para que por lo menos sean controlados.
Muy Alto	60, 64, 75, 80, 100, 125	Son riesgos inaceptables y los Propietarios de los activos deben ser orientados para que los mitiguen inmediatamente.

Fuente: Elaboración Propia

Ya definida la metodología de trabajo, procederemos a obtener la información necesaria y poder realizar los cálculos.

Para ello se ha diseñado un cuestionario el cual será distribuido a los usuarios pertenecientes al **Comité SGSI del Banco Financiero** dado que se trata de usuarios expertos que tienen conocimientos relevantes sobre Riesgos y el Negocio. A continuación, podremos ver gráficamente la estructura:

Figura N° 21 : Organigrama de Lideres Seguridad de Información



Fuente: Elaboración Propia

Para efectos del estudio la herramienta que será usada para recopilar la información será una encuesta, la cual ha sido diseñada con preguntas específicas. Esta encuesta será distribuida a los usuarios pertenecientes a los equipos de la pirámide descrita en el Grafico anterior.

Figura N° 22 : Modelo de Cuestionario

ENCUESTA DE TESIS

El presente cuestionario tiene como finalidad poder recabar información relevante en relación a la investigación '' DISEÑO PARA LA AUTOMATIZACION DEL MANTENIMIENTO DE USUARIOS EN EL PROCESO DE CESES Y LA REDUCCION DEL RIESGO DE FUGA DE INFORMACION EN EL BANCO FINANCIERO DEL PERU''

Marcar con una letra **X** el valor que usted considere el más adecuado en Base a su conocimiento y experiencia

VARIABLE RELEVANCIA. - Se define Relevancia como el valor que el activo de Información tiene para la Organización

Para las siguientes preguntas manejaremos la siguiente Escala:

Valor				
5 Muy Alto	4 Alto	3 Medio	2 Bajo	1 Muy Bajo
Tendría un impacto muy alto o muy grave en la Organización.	Tendría un impacto alto o grave en la Organización.	Tendría un impacto medio en la Organización.	Este tendría un impacto bajo en la Organización.	Tendría un impacto muy bajo o insignificante en la Organización.

Fuente: Elaboración Propia

RELEVANCIA: RESULTADOS DE LA ENCUESTA

Población: 30 Usuarios

Tabla N° 13 : Variable Relevancia Resultados de Encuesta

Usuario	Criterio			Relevancia
	C	I	D	
	Confidencialidad	Integridad	Disponibilidad	(C+D+I)/3
1	5	5	5	5
2	5	5	5	5
3	5	4	5	4.666666667
4	4	5	5	4.666666667
5	5	5	5	5
6	5	5	5	5
7	5	5	4	4.666666667
8	5	4	5	4.666666667
9	5	4	5	4.666666667
10	5	5	4	4.666666667
11	5	4	5	4.666666667
12	5	5	4	4.666666667
13	5	4	5	4.666666667
14	5	5	4	4.666666667
15	5	5	4	4.666666667
16	4	4	4	4
17	5	4	4	4.333333333
18	4	4	5	4.333333333
19	4	5	5	4.666666667
20	4	5	5	4.666666667
21	5	5	5	5
22	5	5	5	5
23	5	4	5	4.666666667
24	5	5	4	4.666666667
25	5	4	4	4.333333333
26	4	4	5	4.333333333
27	5	5	4	4.666666667
28	5	4	5	4.666666667
29	4	5	5	4.666666667
30	5	5	4	4.666666667
			Promedio	**4.66**

Fuente: Elaboración Propia

IMPACTO: RESULTADOS DE LA ENCUESTA

Tabla N° 14 : Variable Impacto Resultados de Encuesta

Usuario	Criterio					Relevancia
	IP	OL	S	FC	PC	
	Información Personal	Obligaciones Legales	Seguridad	Factores Comerciales	Pérdida de Confianza	(IP+OL+S+FC+PC+D+I)/5
1	5	5	4	5	5	4.8
2	4	4	4	4	5	4
3	4	4	4	4	5	4
4	4	4	4	5	5	4
5	4	4	4	5	5	4
6	4	4	4	4	5	4
7	4	4	5	4	5	4.333333333
8	5	4	4	4	5	4.333333333
9	4	4	4	4	5	4
10	5	4	5	5	5	4.666666667
11	4	5	4	5	5	4.333333333
12	5	4	4	4	5	4.333333333
13	5	4	5	5	5	4.666666667
14	4	4	4	4	5	4
15	4	4	4	5	5	4
16	4	4	4	5	5	4
17	4	5	4	4	5	4.333333333
18	4	5	5	4	5	4.666666667
19	5	5	4	4	5	4.666666667
20	4	4	5	5	5	4.333333333
21	5	4	4	4	5	4.333333333
22	4	4	5	5	5	4.333333333
23	5	4	4	4	5	4.333333333
24	4	5	5	5	5	4.666666667
25	5	5	4	5	5	4.666666667
26	4	4	4	5	5	4
27	5	5	4	5	5	4.666666667
28	5	4	4	4	5	4.333333333
29	4	4	4	4	5	4
30	4	5	4	4	5	4.333333333
					Promedio	4.304444444

Fuente: Elaboración Propia

PROBABILIDAD: RESULTADOS DE LA ENCUESTA

Tabla N° 15 : Variable Probabilidad Resultados de Encuesta

Usuario	Frecuencia Anual
1	3
2	4
3	4
4	3
5	4
6	4
7	3
8	3
9	5
10	4
11	4
12	4
13	5
14	4
15	5
16	3
17	3
18	4
19	4
20	4
21	4
22	3
23	4
24	4
25	4
26	4
27	3
28	5
29	4
30	4
Promedio	**3.866666667**

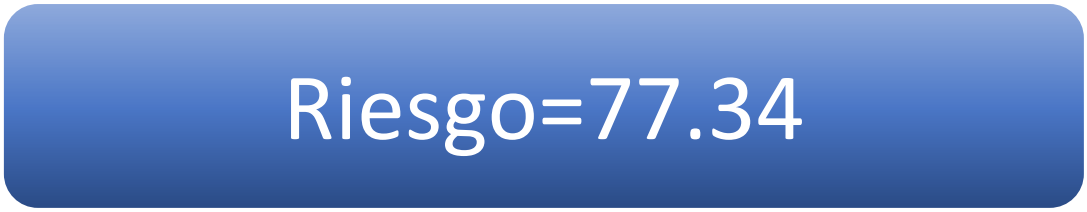
Fuente: Elaboración Propia

Con toda la información recopilada en las encuestas respecto a cada variable, tenemos en resumen los siguientes valores:

Valoración Promedio: 4.66

Impacto Promedio: 4.30

Probabilidad Promedio: 3.86



Contrastando con Nuestra escala de Nivel de Riesgo, este valor encaja en el Nivel de Riesgo Muy Alto:

Tabla N° 16 : Riesgo Calculado Versus Nivel de Riesgo

Nivel de Riesgo de Control PSR		Riesgo Calculado	Acciones a Tomar
Nivel de Riesgo	Rango de Valores P*S*R		
Muy Alto	60, 64, 75, 80, 100, 125	**77.34**	Son riesgos inaceptables y los Propietarios de los activos deben ser orientados para que los mitiguen inmediatamente.

Fuente: Elaboración Propia

Actualmente en Base a la información obtenida hemos calculado que el Riesgo de Fuga de Información bajo el Proceso de Ceses Actual tienen un valor de: **77.34**

Este valor encaja dentro de nuestra escala de nivel de Riesgo como un **Riesgo Muy Alto que debe ser mitigado** y se necesita aplicar un control o mejorar la eficacia del control Actual.

Acorde a la investigación, nuestro objetivo Principal es demostrar que, con el nuevo Diseño Para La Automatización Del Mantenimiento De Usuarios en el Proceso De Ceses, el riesgo de Fuga de Información deberá mitigarse y el Nivel de Riesgo que actualmente según la escala corresponde a Muy Alto deberá cambiar a un Nivel Medio o Bajo.

3.2. DESARROLLO DEL NUEVO DISEÑO DEL PROCESO DE CESES

La propuesta del Nuevo Diseño del Proceso de Ceses, está orientado a automatizar algunas tareas que actualmente dentro del Flujo se ejecutan de forma manual. Esto trae como consecuencia inversión de tiempo elevado, errores operativos y un alto riesgo de fuga de información por los tiempos que en algunos casos pueden excederse por varios factores.

Si bien es cierto la automatización de tareas actualmente puede ser implementada a través de diversas herramientas, tanto Open Source o Licenciadas; para la presente investigación vamos a utilizar conceptos y herramientas con las que el Banco actualmente cuenta pero que sin embargo no han sido explotadas.

Para que el nuevo diseño automatizado del Proceso propuesto funcione, uno de los primeros pasos será estandarizar la información que servirá como input para el Nuevo Proceso.

A continuación, se detalla paso a paso las actividades a ejecutar:

3.2.1. NOTIFICACION DE CESE

Como punto de partida tenemos la Actividad de Notificación de Cese, esta información es enviada desde Gestión de Personas hacia Seguridad TI – Control de Accesos y la cual se realiza de forma manual a través de correo el electrónico.

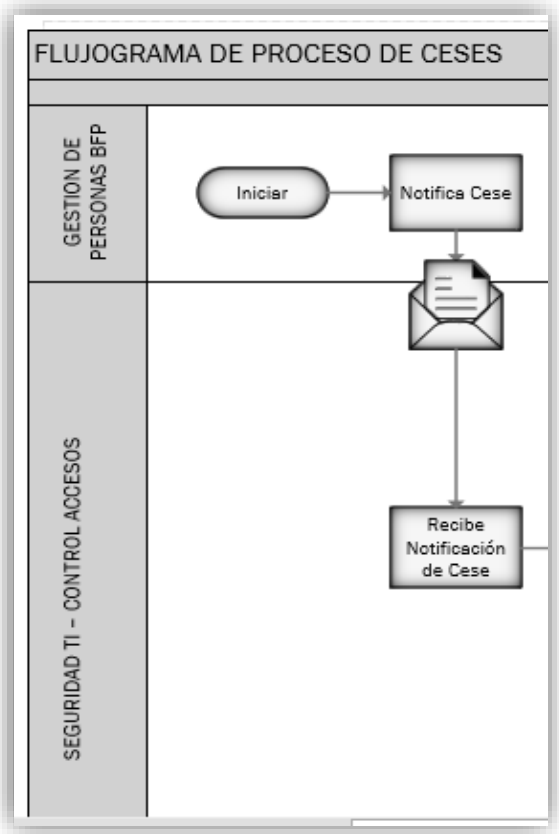
Los campos de la información del colaborador enviada actualmente es la siguiente:

Tabla N° 17 : Información de Usuario enviada en Notificación de Cese

CÓDIGO EMPLEADO	NOMBRE COMPLETO	CARGO	FECHA DE CESE
6173	Joel Acosta	ANALISTA DE SEGURIDAD	31/10/2015

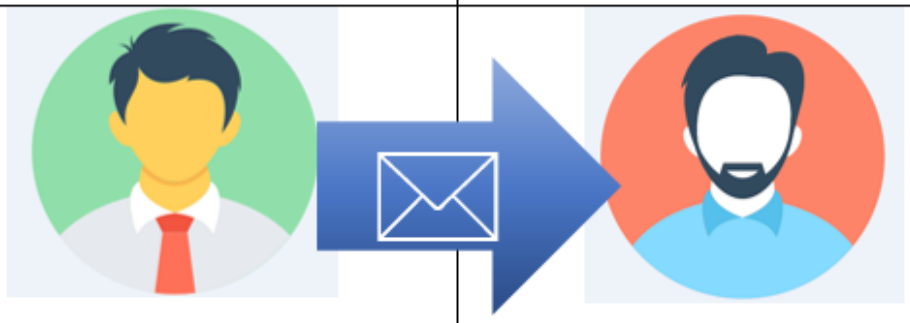
Fuente: Elaboración Propia

Figura N° 23: Flujograma de Notificación de Cese



Fuente: Elaboración Propia

Figura N° 24 : Trazabilidad de Notificación de Cese

GESTION DE PERSONAS	SEGURIDAD TI
	
El área de Remuneraciones en coordinación con las áreas internas de la Gerencia de Gestión de Personas , notifica vía correo electrónico los datos según plantilla mostrada de los colaboradores que pasarán al estado Cesado	Seguridad TI – Control de Accesos , recibe la notificación y procede a dar de Baja las cuentas de usuario creadas en las aplicaciones críticas definidas por el Banco Financiero.

Fuente: Elaboración Propia

Propuesta de Mejora

Dentro del nuevo diseño debemos empoderar y en coordinación con el equipo de Gestión de Personas, a la información que se envía actualmente para el colaborador que será cesado se añadirá 2 nuevos Datos. Estos datos corresponden al Número de DNI y correo corporativo:

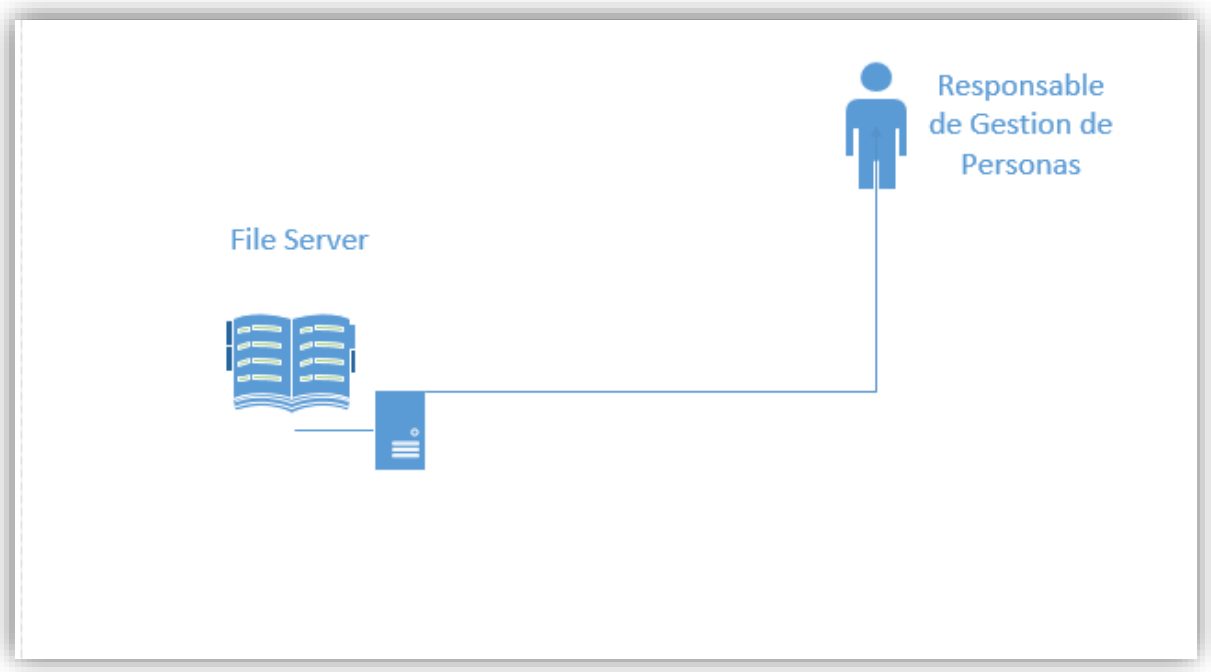
Tabla N° 18 : Nuevos Datos de Usuario en Notificación de Cese

CÓDIGO EMPLEADO	NOMBRE COMPLETO	CARGO	FECHA DE CESE	DNI	Correo Corporativo
6173	Joel Acosta	ANALISTA DE SEGURIDAD	31/10/2015	44436571	Jorge.acosta@financiero.pe

Fuente: Elaboración Propia

Se propone que la notificación ya no sea enviada a través de correo electrónico. Lo que se creará es un repositorio compartido en un File Server, en donde Gestión de Personas depositará la información de usuarios a ser Cesados.

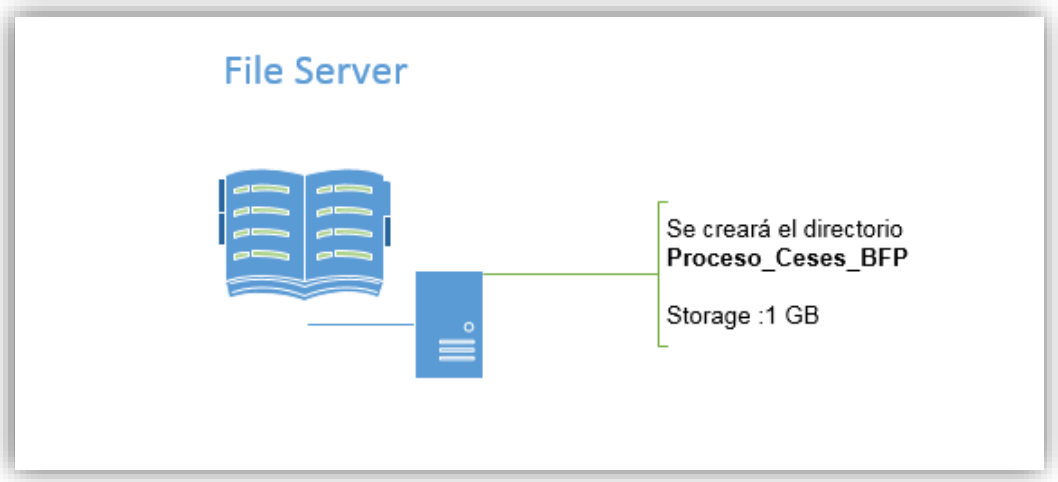
Figura N° 25 : Nuevo Diseño de Notificación de Cese



Fuente: Elaboración Propia

Se creará un directorio reservado en el File Server será usado para el Proceso de Ceses, este directorio lo denominaremos como: **Proceso_Ceses_BFP.**

Figura N° 26: Directorio Reservado en File Server



Fuente: Elaboración Propia

A este directorio se la brindará los siguientes permisos:

Responsable GP: Owner

Serán administradores de la carpeta y ellos podrán darle mantenimiento de los permisos Adicionar o remover usuarios.

Responsable Seguridad TI: Lectura, Escritura

Para efectos de revisiones por Incidentes reportados.

Responsable de Seguridad de Información: Lectura

Para efectos de Auditoría

Usuario de Servicio: Owner

Este usuario será creado para la configuración del sistema.

3.2.2. EJECUCION DEL CESE

Actualmente la ejecución de la Baja de Usuarios en los distintos sistemas del Banco Financiero se realiza de forma manual. En el capítulo anterior se calculó que la ejecución del Cese de 1 solo colaborador en promedio representa 25 minutos

Propuesta de Mejora

La propuesta se centra en automatizar el mantenimiento de Usuarios en el Proceso de Ceses y cuyo alcance solo es sobre 4 aplicaciones críticas definidas por el Banco Financiero:

Figura N° 27 : Aplicaciones Críticas del Banco Financiero

Fuente: Elaboración Propia

¿Cómo se automatizará la ejecución de las Bajas?

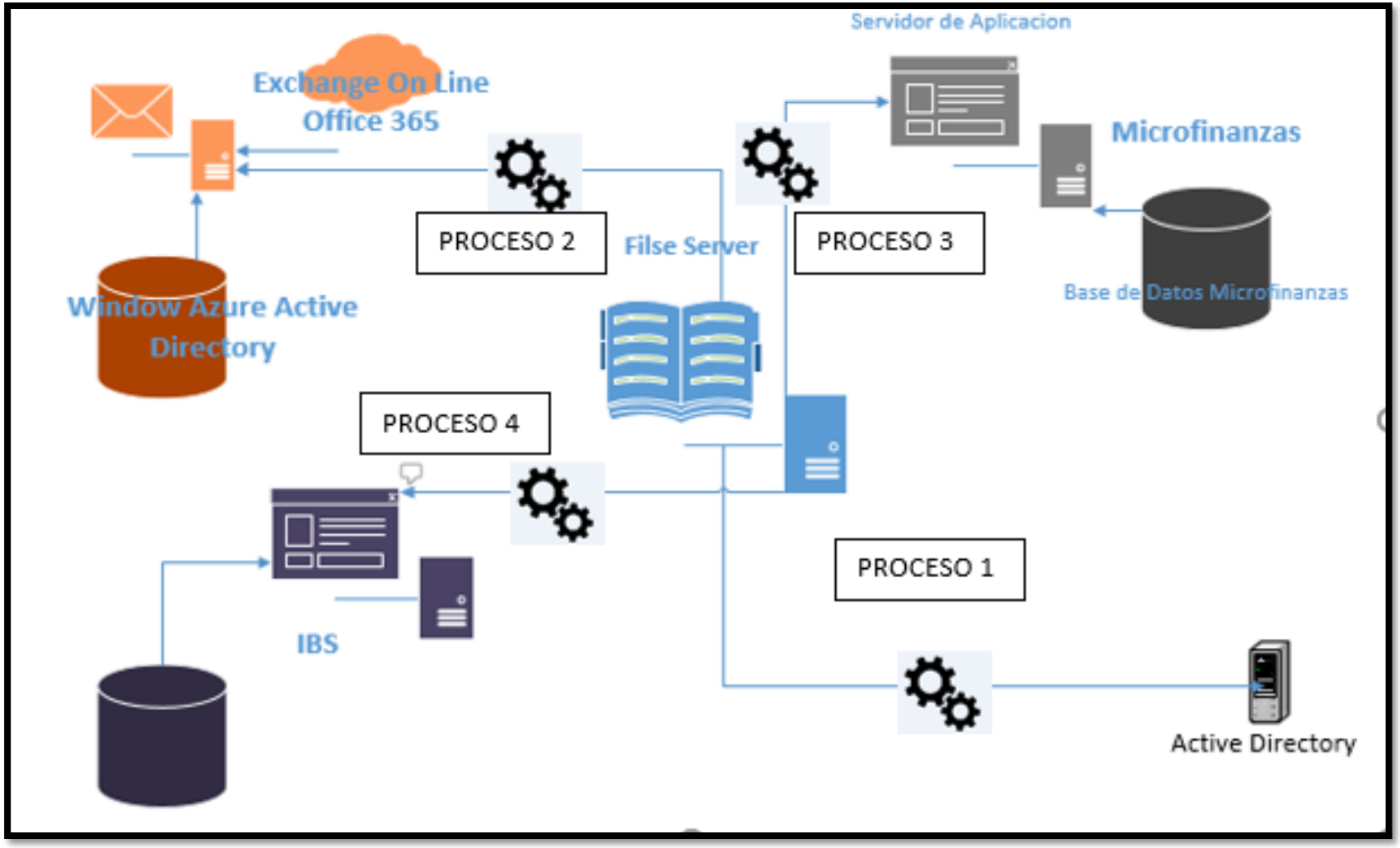
En el presente estudio, el nuevo diseño del mantenimiento de usuarios para el Proceso de Ceses será automatizado; sin embargo, solo podrán automatizarse algunas tareas dentro de todo el Flujo de actividades que se realizan.

La generación del ticket en el CA Service Desk, el envío de la respuesta de la ejecución de los Ceses por correo y el llenado de la Bitácora de Ceses, continuarán siendo tareas que deberán ser ejecutadas manualmente. Los esfuerzos invertidos en estas tareas corresponden a 11 minutos de esfuerzo del Total.

Las actividades que serán automatizadas, son la ejecución de la baja de los usuarios en cada módulo de Seguridad de las aplicaciones críticas definidas por el negocio y descritas anteriormente. Al ser aplicaciones que no tienen en común el diseño de la Base de Datos, tampoco la plataforma en las cuales fueron desarrolladas, vamos a trabajar en programas independientes en base al análisis de cada uno de los sistemas para conocer sus limitantes y las oportunidades de explotar herramientas que más se adecuen a los objetivos.

Estos programas se alimentarán de un archivo donde se registrará la información de los usuarios que deben ser dados de Baja y será depositado en el directorio **Proceso_Ceses_BFP** creado en File Server reservado para este Proceso. Este archivo será actualizado por el responsable de Gestión de Personas con información cada vez que exista un colaborador que deba ser Cesado y a través de tareas programadas configuradas en los servidores se ejecutarán los programas creados con un algoritmo que leerá el archivo y validará la fecha de Cese.

Figura N° 28 : Nuevo Diseño del Mantenimiento de Usuarios en el Proceso de Ceses



Fuente: Elaboración Propia

A través de 4 Procesos programados para ser ejecutados de forma periódica, estaríamos automatizando el Mantenimiento de Usuarios en el Proceso de Ceses.

1. El programa tendrá un algoritmo configurado para que sea ejecutado todos los días a las 06:30 pm.
2. Será desarrollada en la herramienta más adecuada de acuerdo al sistema: Power Shell, C#, SQL Server.
3. El archivo de usuarios Cesados no deberá cambiar de nombre dado que estará configurado en los programas.
4. El algoritmo validará la fecha del Cese para su ejecución.

A continuación, se detalla cada Proceso y la forma como sería implementado:

PROCESO 1.- MANTENIMIENTO DE USUARIOS DE RED

Para poder cumplir con la Baja de Usuarios de Red, debemos seguir dos pasos:

1. Deshabilitar la cuenta de red del usuario en el Active Directory.
2. Mover el Objeto ‘’User’’ ala OU = Unidad Organizativa ´´Ex Financiero´´

Para ello nos soportaremos en la programación por **Power Shell,** que contiene cmlet's (comandos) que nos facilitarán la codificación.

La estructura de la Programación contará de 4 Fases:

1. Se armará la plantilla del archivo CSV, en base al archivo centralizado en el File Server: **Proceso_Ceses_BFP**. Para ello, Seguridad TI deberá revisar la carpeta de forma periódica antes de las 06:30 pm y de encontrar información actualizada procederá a cambiar el formato.

   Debemos asegurarnos que el archivo de texto tenga una estructura de Datos lógica con los atributos de los usuarios del Active Directory y los registros en cada línea, sin espacio entre las líneas, por ejemplo:

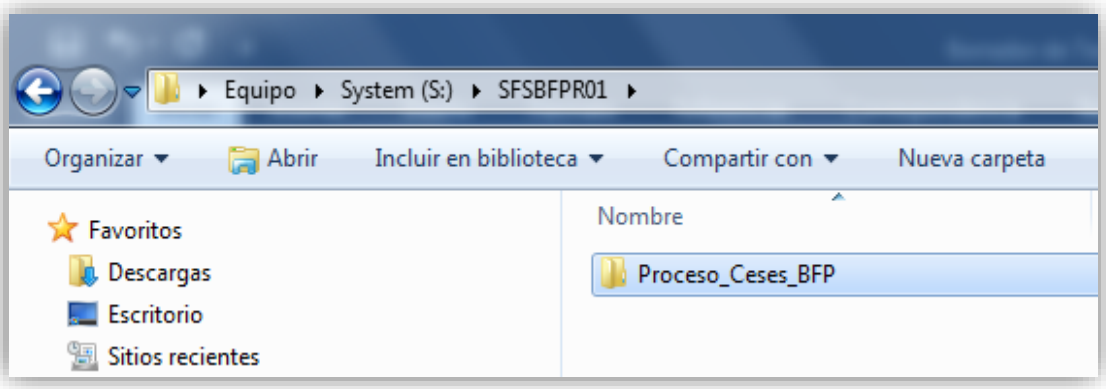
   Para esta investigación estamos tomando el atributo **Initial** del Active Directory que en la práctica representa el Código de Colaborador del Banco Financiero, como el Dato que servirá de llave para la ejecución del Script.

   Ejemplo:

   Tenemos el Directorio en el File Server:

   Aquí se muestra el Directorio creado en el Servidor de Archivos

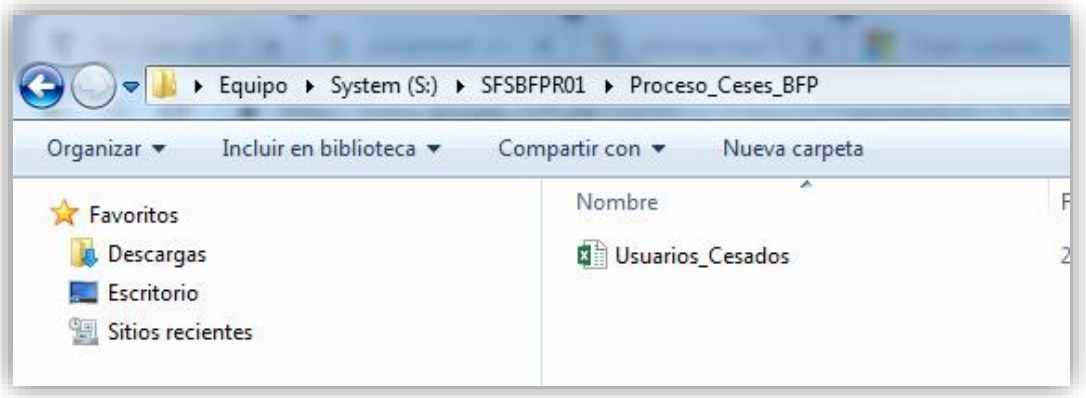
Figura N° 29 : Directorio Creado en File Server para Proceso de Ceses



Fuente: Elaboración Propia

Archivo con Datos de los usuarios que deberán ser Cesados: Esta es la información que depositará Gestión de Personas en el Directorio Compartido.

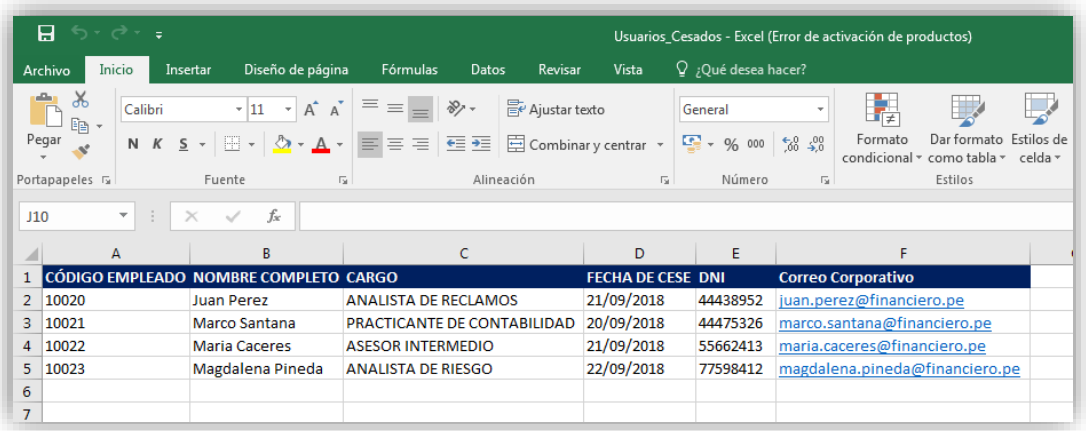
Figura N° 30 : Archivo de Registro de Usuarios Cesados



Fuente; Elaboración Propia

Archivo con los Registros y Campos que contiene la información de los Usuarios que deberán ser Cesados.:

Figura N° 31 : Campos Requeridos de Usuarios Cesados

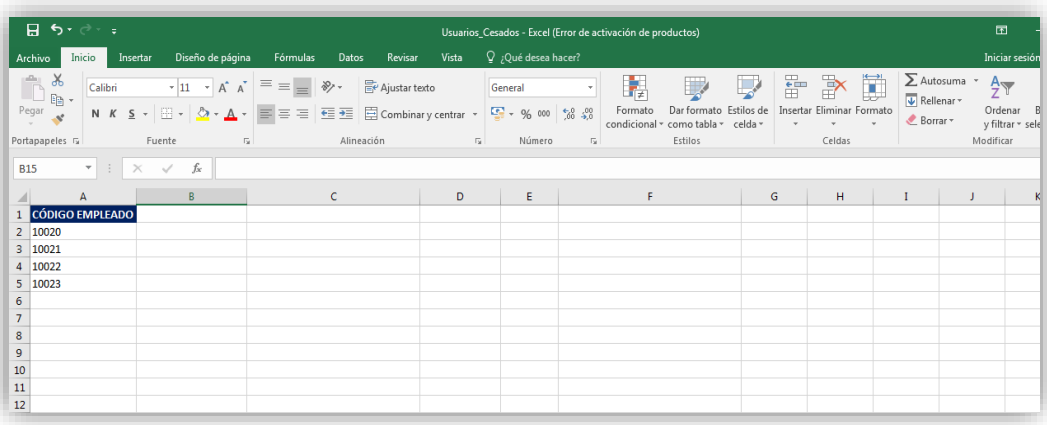


	A	B	C	D	E	F
1	CÓDIGO EMPLEADO	NOMBRE COMPLETO	CARGO	FECHA DE CESE	DNI	Correo Corporativo
2	10020	Juan Perez	ANALISTA DE RECLAMOS	21/09/2018	44438952	juan.perez@financiero.pe
3	10021	Marco Santana	PRACTICANTE DE CONTABILIDAD	20/09/2018	44475326	marco.santana@financiero.pe
4	10022	Maria Caceres	ASESOR INTERMEDIO	21/09/2018	55662413	maria.caceres@financiero.pe
5	10023	Magdalena Pineda	ANALISTA DE RIESGO	22/09/2018	77598412	magdalena.pineda@financiero.pe
6						
7						

Fuente: Elaboración Propia

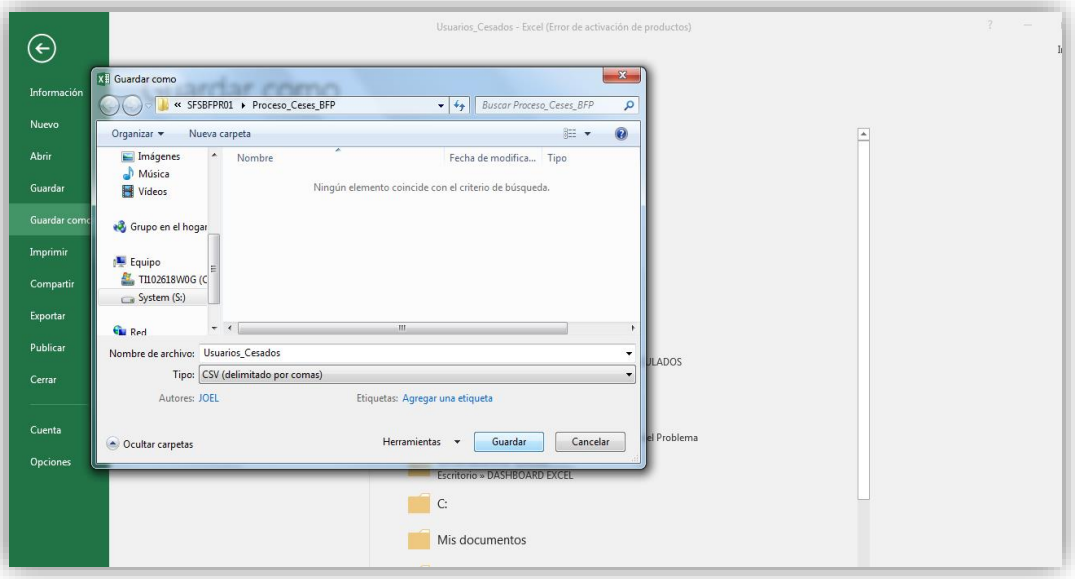
Seguridad TI modifica el Archivo solo con los campos necesarios y lo guarda en formato **.csv**

Figura N° 32 : Archivo Formato CSV



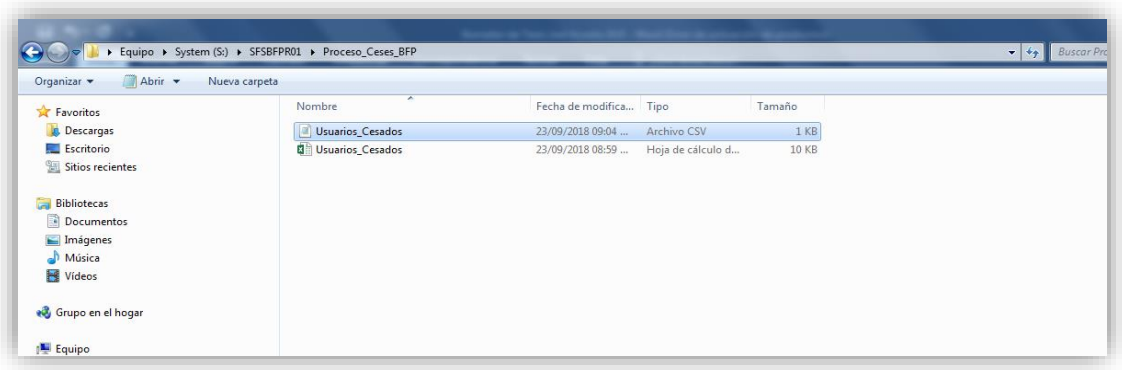
Fuente: Elaboración Propia

Figura N° 33 : Proceso de Guardado de Archivo en CSV



Fuente : Elaboración Propia

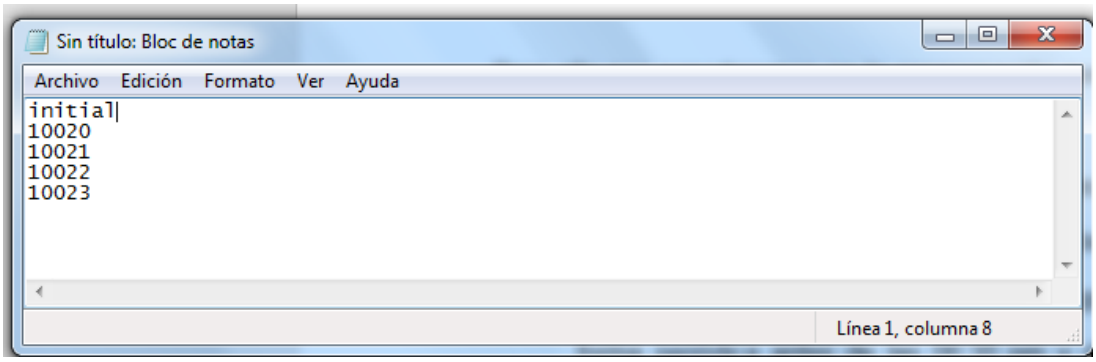
Figura N° 34 : Archivo Depositado en Directorio de File Server



Fuente: Elaboración Propia

Aquí se puede observar el formato final del archivo.

Figura N° 35 : Archivo CSV con Datos de Usuarios Cesados



Fuente: Elaboración Propia

2. Se construirá el Script para la Des habilitación Masiva de Usuarios.

   El Script, su funcionamiento es recorrer cada línea del archivo csv donde debería estar el atributo Initial del usuario, lo asigna a la variable $Initial y lo deshabilita.

   El atributo Initial es **referencial** dado que puede colocarse en la variable cualquier otro atributo del AD (***samAccountName, DisplayName, NickName, etc.***), siempre

y cuando se considere que el dato debe siempre estar registrado en el Active Directory.

Para la presente investigación nuestra población Objetivo son solo usuarios planilla Banco Financiero y el atributo Initial es registrado de forma obligatoria.

Esta sería la programación del Script en Power Shell, referencial:

Figura N° 36 : Bloqueo de Usuarios en Active Directory Power Shell

```
Import-Module activedirectory //Sirve para llamar a los comandos

$list = Import-CSV c:\Proceso_Ceses_BFP\Usuarios_Cesados.csv // Se asigna los datos del archive CSV a la variable

forEach ($item in $list) {

$Initial = $item.Initial

Disable-ADAccount -Identity $Initial
}// Bucle para la deshabilitacion de las cuentas
```

Fuente: Elaboración Propia

3. Se construirá el Script para Mover los Usuarios hacia la OU

Figura N° 37 : Mover Usuario de OU en Active Directory Power Shell

```
$ListaUsuarios=Get-Content -Path "
c:\Proceso_Ceses_BFP\Usuarios_Cesados.csv "
$TargetOU="OU=ExFinanciero,DC=financiero,DC=bco"
For ($i=0;$i -lt $ListaUsuarios.Count;$i++){
$MoverUsuario=$ListaUsuarios[$i]
$UsuarioAD=Get-ADUser -Filter {Initial -like $MoverUsuario}
Move-ADObject $UsuarioAD.DistinguishedName -TargetPath
$TargetOU
}
```

Fuente: Elaboración Propia

4. Se configurará una tarea programada de Windows en el servidor de Active Directory que ejecute el Script de acuerdo a la programación que se defina. En este caso se plantea que la ejecución sea a las 06:30 pm de forma periódica. A continuación, se muestra el modelo de configuración que se seguirá:

CARACTERÍSTICAS DEL SERVIDOR

IP Privada Referencial: 172.17.X.Y

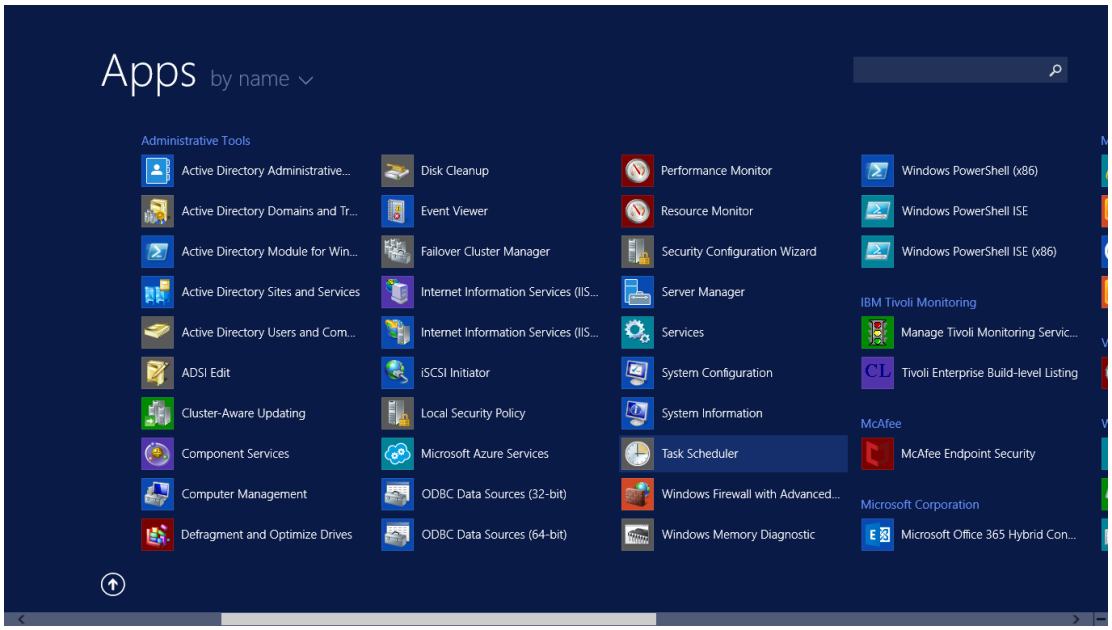
Hostname: SADFINANCIERO

Sistema Operativo: Windows Server 2008 R2

La tarea programada se configurará de la siguiente forma:

Programador de Tareas :

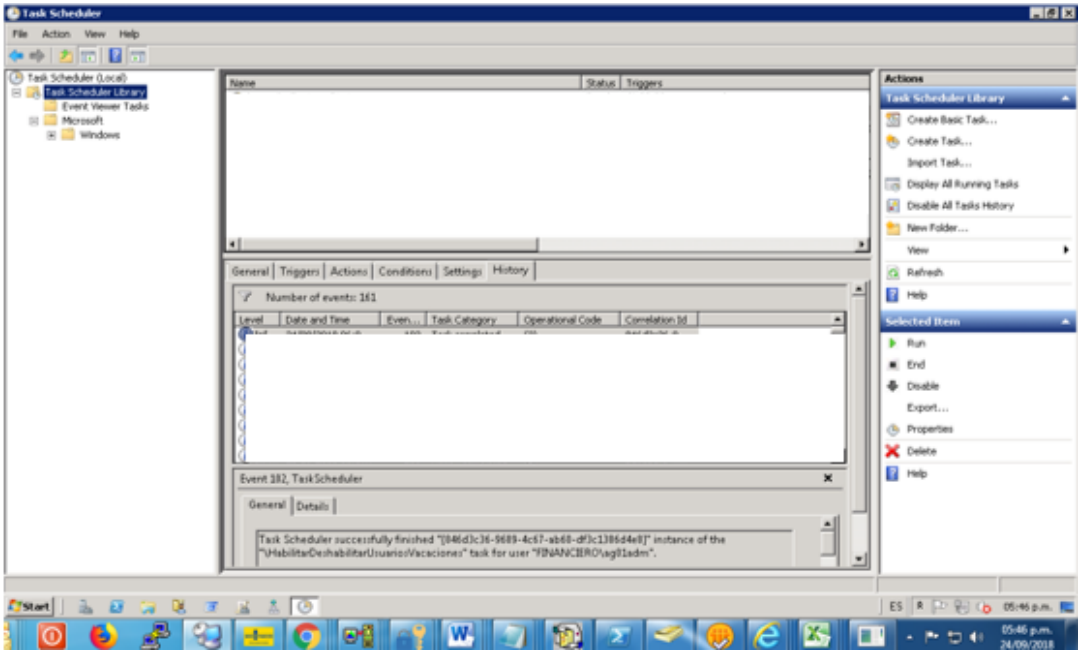
Figura N° 38 : Programador de Tareas Servidor Active Directory



Fuente: Elaboración Propia

Visualizamos la configuración de las tareas:

Figura N° 39 : Panel de Configuración de Programador de Tareas

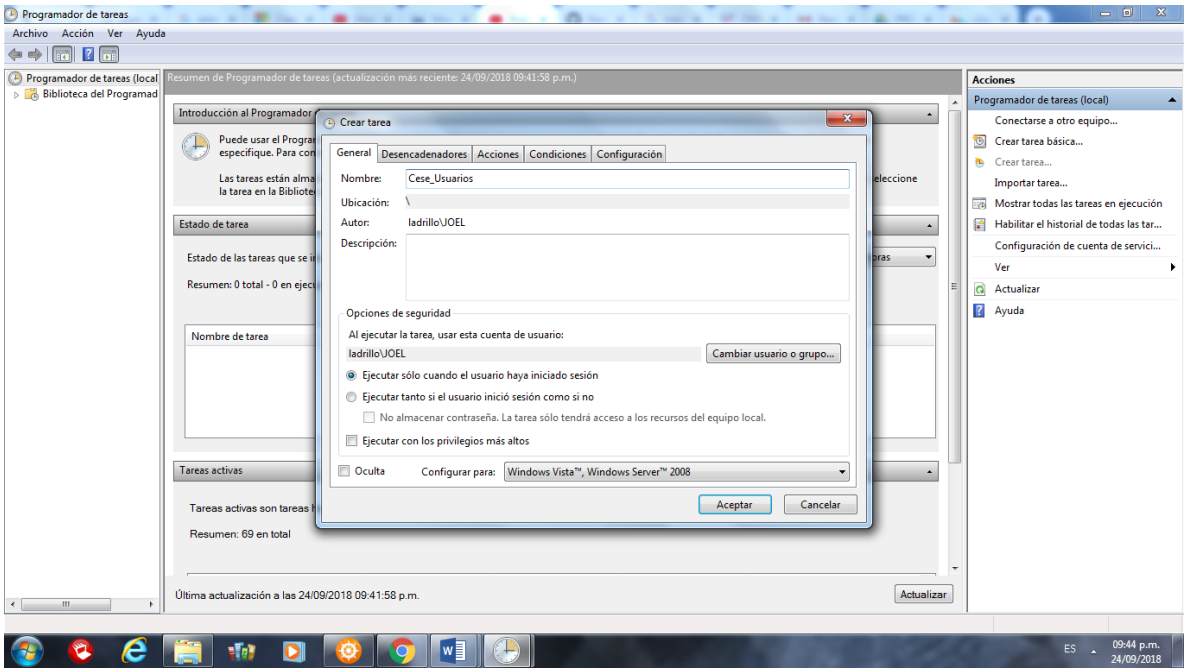


Fuente: Elaboración Propia

Agregamos la Nueva tarea.

- ✓ Primero colocamos un Nombre a nuestra tarea Programada.

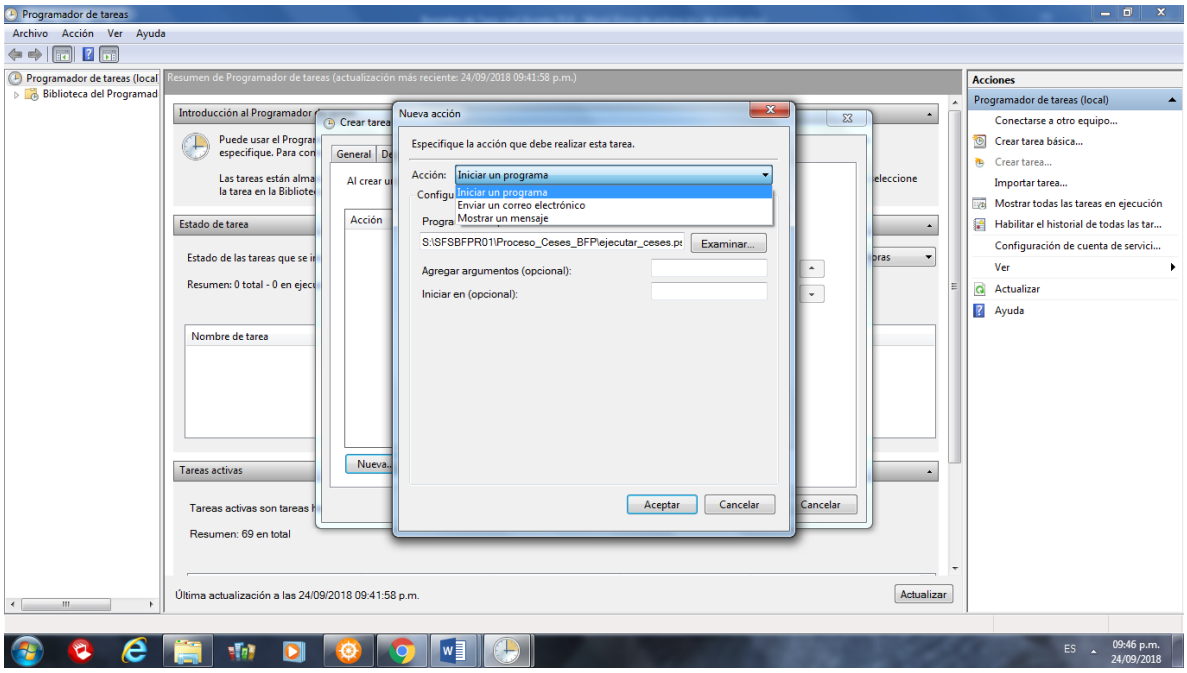
Figura N° 40 : Configurando Nombre de tarea Programada en Servidor Active Directory



Fuente: Elaboración Propia

- ✓ Configuramos las Acciones, en este caso Ejecutar un Programa o Script

Figura N° 41 : Configuración de Script en Programador de Tareas

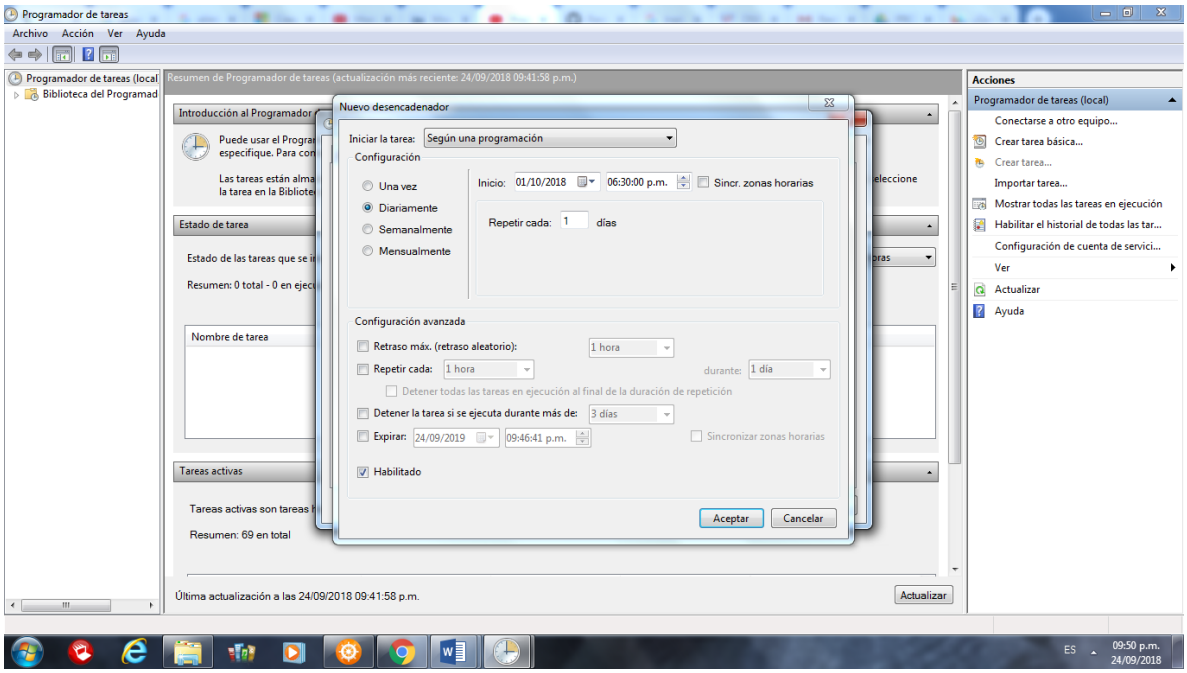


Fuente: Elaboración Propia

✓ Luego configuramos el Desencadenador:

Figura N° 42 : Configuración de Desencadenador

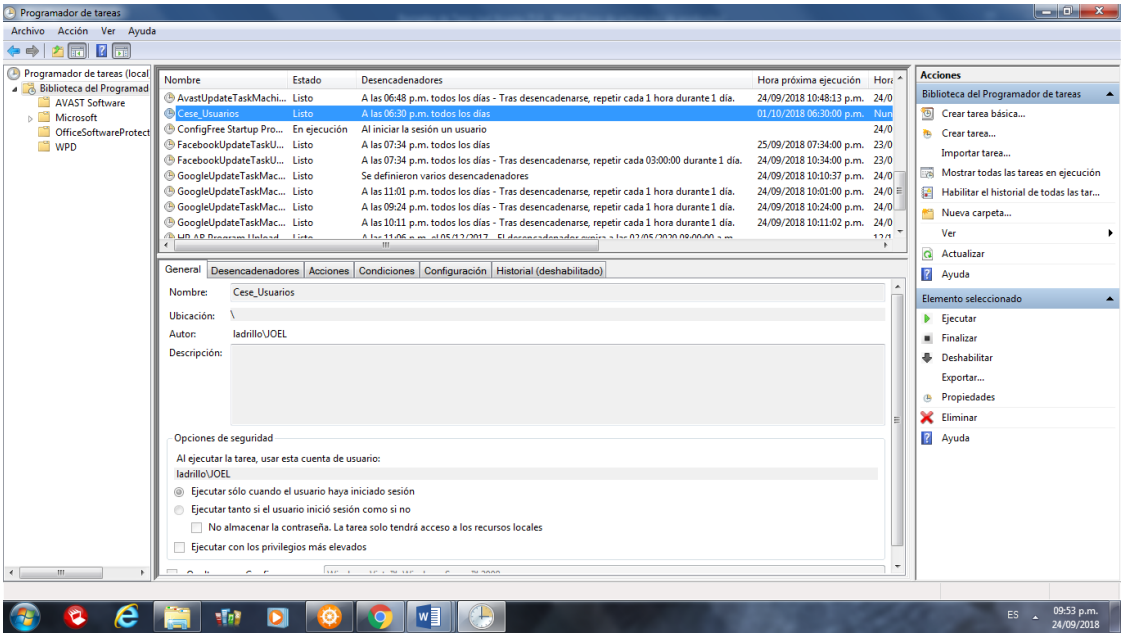
en Programador de tareas



Fuente: Elaboración Propia

✓ Guardamos y la tarea ya está programada:

Figura N° 43 : Tarea Programada Configuración de Nombre



Fuente: Elaboración Propia

PROCESO 2.-MANTENIMIENTO DE USUARIOS EN EL CORREO ELECTRÓNICO.

Como ya se había explicado, el Banco Financiero actualmente mantiene una arquitectura hibrida respecto al correo electrónico, se tienen cuentas On Premise creadas en Exchange Server, Cuentas de correo electrónico Hibridas (Migradas) a Exchange On Line.

Para automatizar este Proceso, utilizaremos la programación basada en **Power Shell** que contiene los cmlets necesarios para ejecutar la tarea de forma masiva.

Debemos tener presente que la configuración actual de la plataforma de correo esta sincronizada con nuestro Active Directory, y existe la Unidad Organizativa **OU Ex financiero** que no sincroniza con Exchange On Line.

¿Qué quiere decir esto?

Que todos los Objetos de Tipo ‘’**User**’’ que sean movidas al contenedor Ex Financiero ya no estarán sincronizadas hacia Exchange On Line, por ende, el buzón de correo con Licencia que figura en Exchange On Line se deshabilitará de forma automática.

Sin embargo, queda en estado huérfano Objetos en Exchange Server que no comprometen el acceso al correo, pero están utilizando espacio del BD y es necesario que sean deshabilitados.

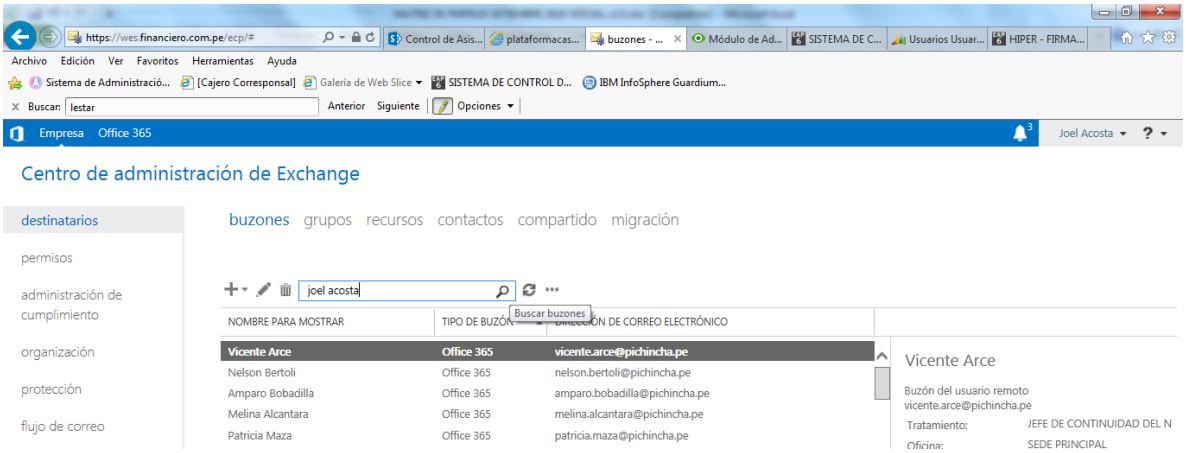
Para ello utilizaremos la herramienta Exchange Management Shell y a través del uso de comandos deshabilitaremos estos Objetos.

Figura N° 44 : Comando para Deshabilitar Objetos Exchange Server

```
Comando Referencial: Disable-Mailbox ‘’……’’
```

Fuente: Elaboración Propia

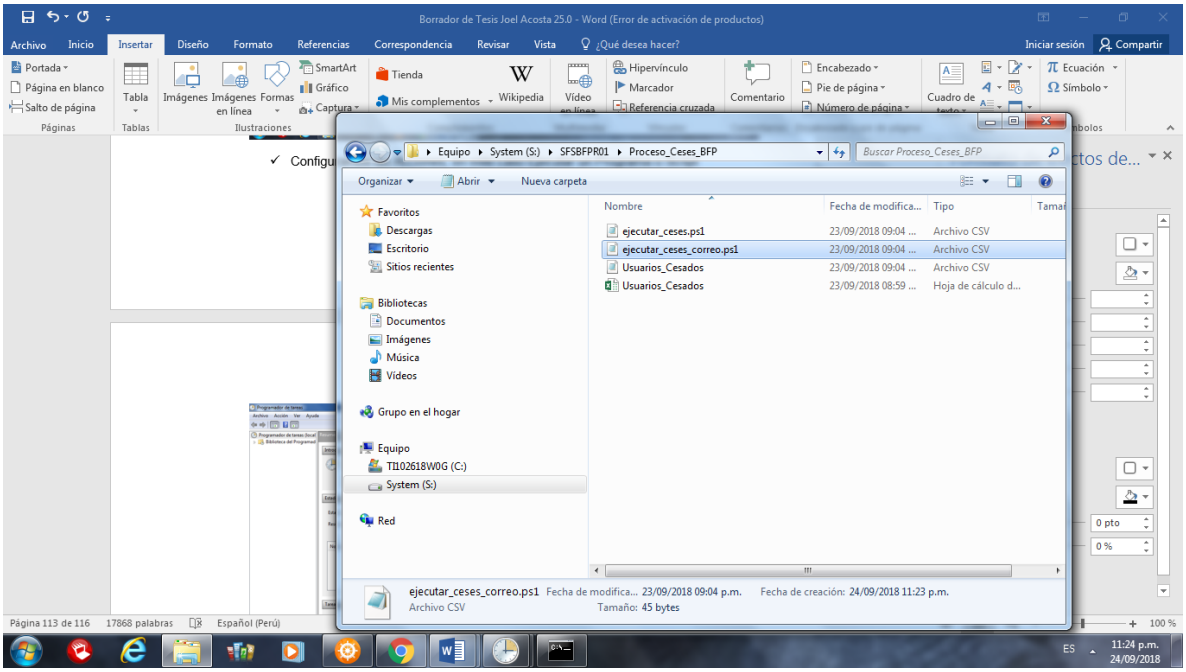
Figura N° 45 : Objetos Tipo Buzón de Usuario



Fuente: Elaboración Propia

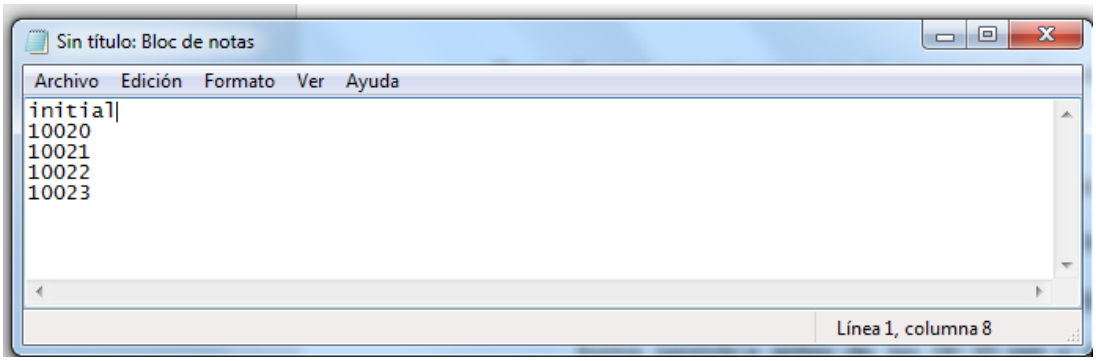
El Script utilizará como input el archivo **Usuarios_Cesados** del directorio **Proceso_Cese_BFP**.

Figura N° 46 : Directorio y Archivo de Ceses en File Server



Fuente: Elaboración Propia

Figura N° 47 : Archivo Formato Texto Plano



Fuente: Elaboración Propia

Una vez que Script se ejecuta los Buzones de Usuarios, serán deshabilitados.

De igual forma en el Servidor Exchange se deberá configurar una tarea programada:

CARACTERÍSTICAS DEL SERVIDOR

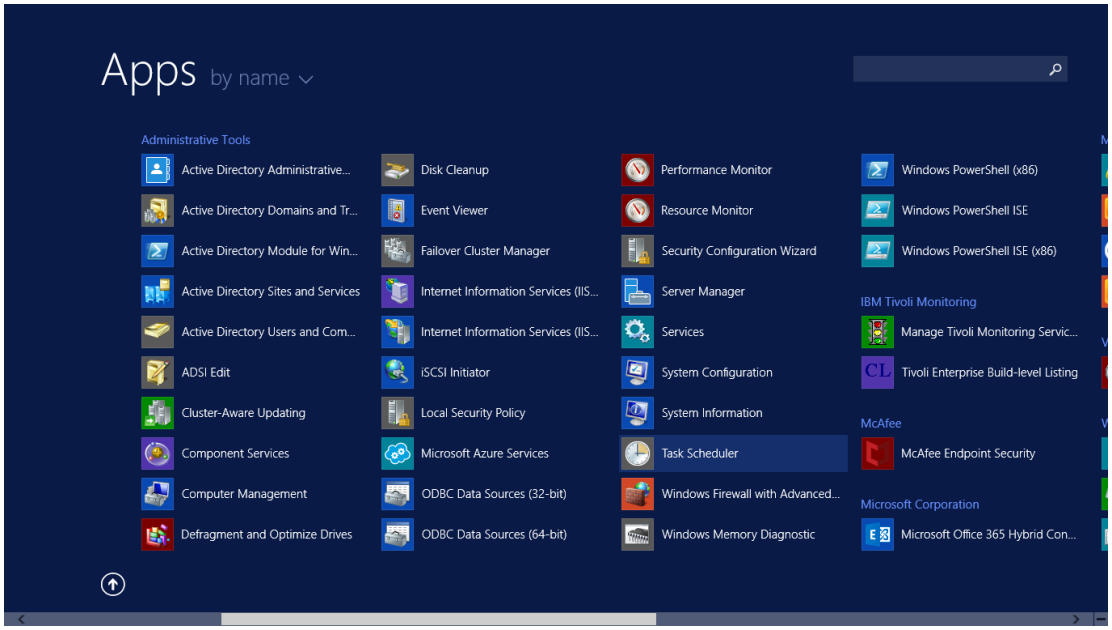
IP Privada Referencial: 172.17.Z.P

Hostname: SMEFINANCIERO

Sistema Operativo: Windows Server 2012 R2

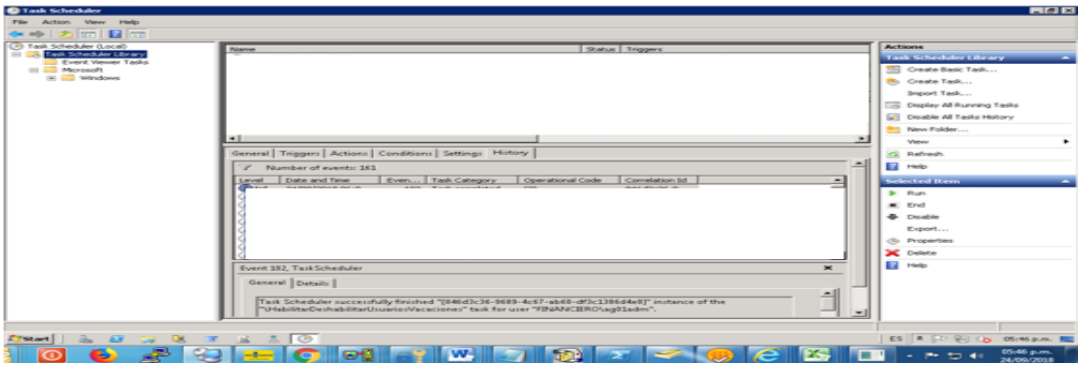
La tarea programada se configurará de la siguiente forma:

Figura N° 48 : Programador de tareas Exchange Server



Fuente: Elaboración Propia

Figura N° 49 : Panel de Configuración Programador de Tareas

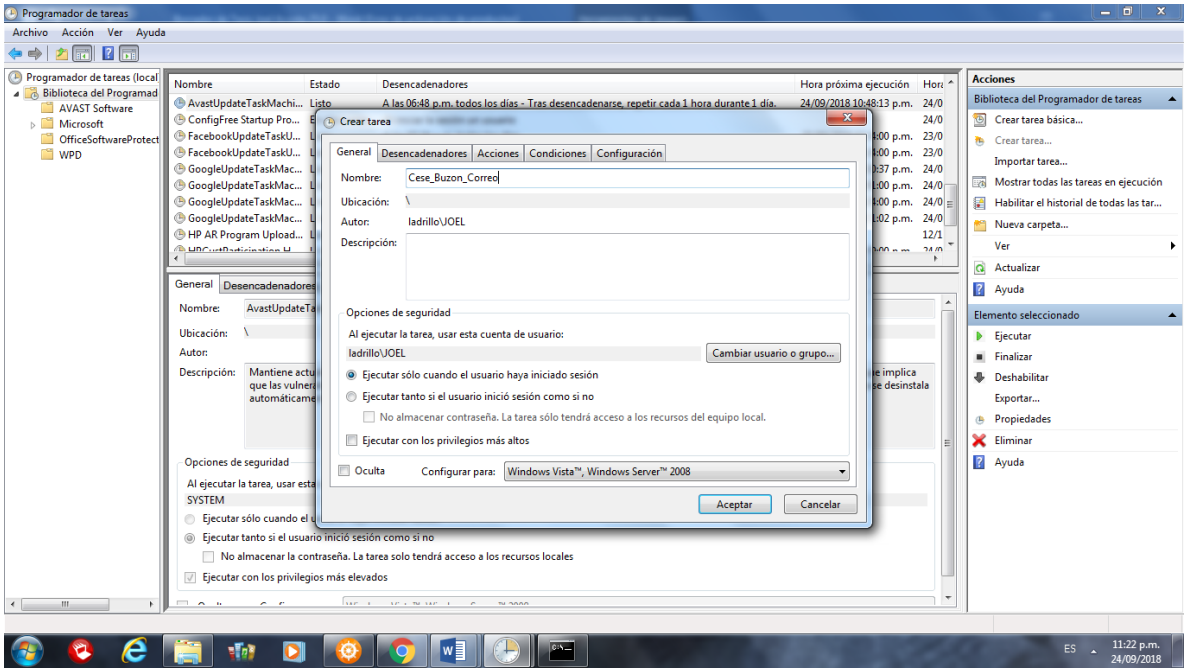


Fuente: Elaboración Propia

Agregamos la Nueva tarea.

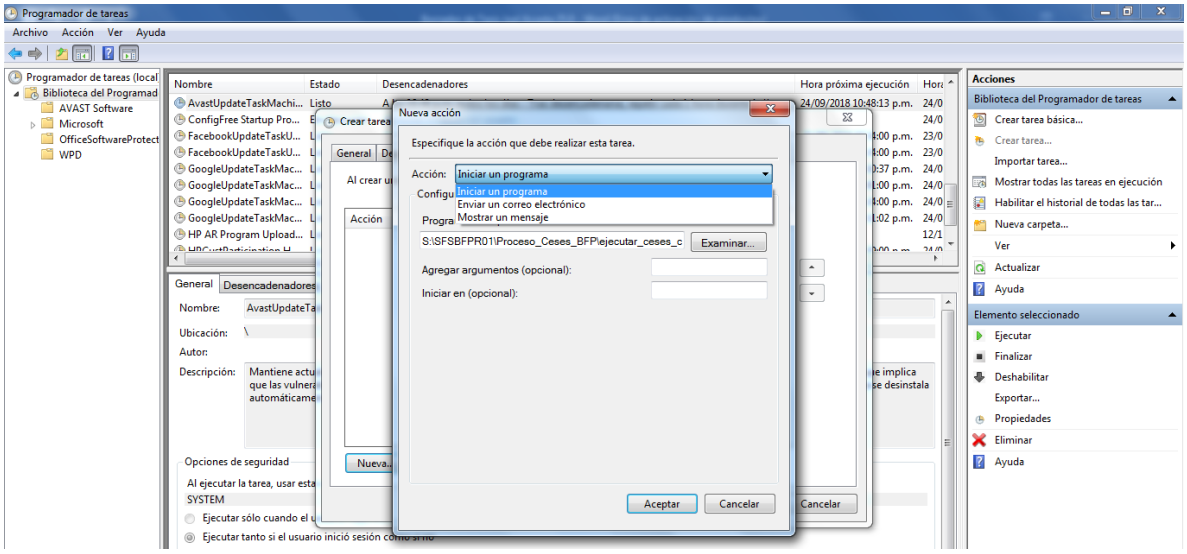
- ✓ Primero colocamos un Nombre a nuestra tarea Programada.

Figura N° 50 : Configuración Nombre Tarea programada Exchange Server



Fuente: Elaboración Propia

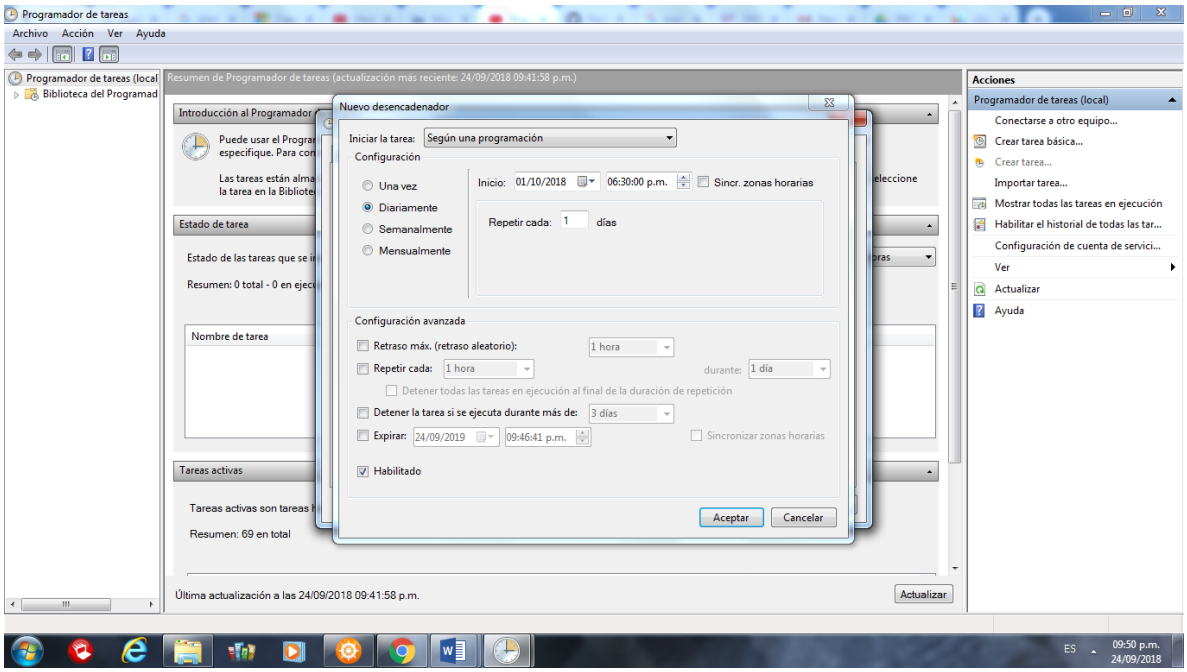
Figura N° 51 : Configuración Accion en Exchange Server



Fuente: Elaboración Propia

✓ Luego configuramos el Desencadenador:

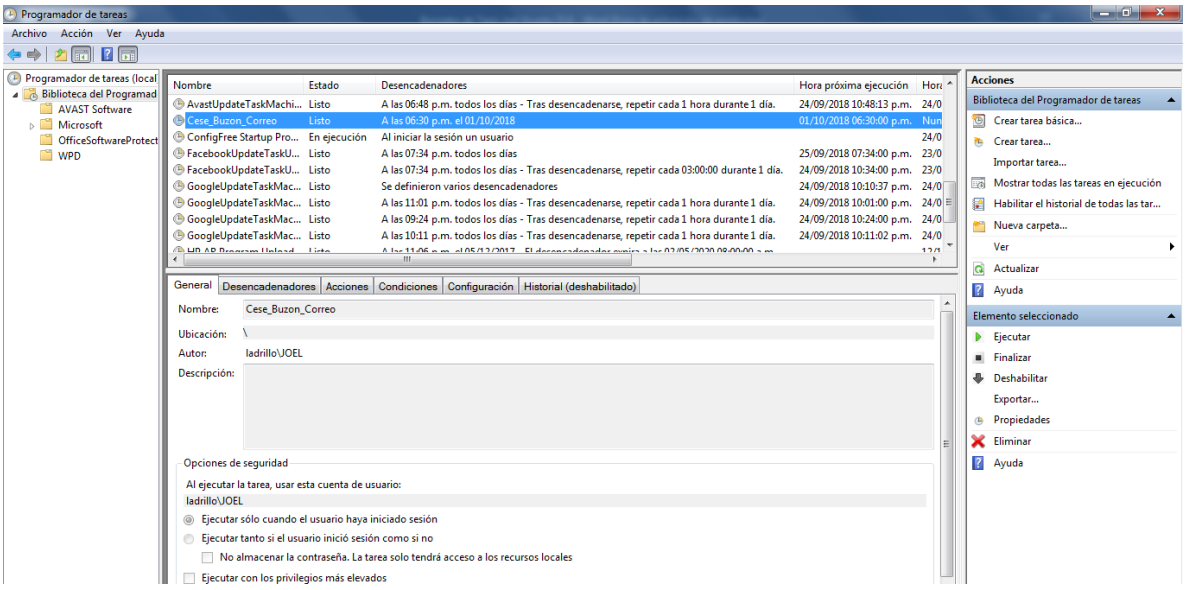
Figura N° 52 ; Configuración Desencadenador Exchange Server



Fuente: Elaboración Propia

✓ Guardamos y la tarea ya está programada:

Figura N° 53 : Tarea Programada Configurada Exchange Server



Fuente: Elaboración Propia

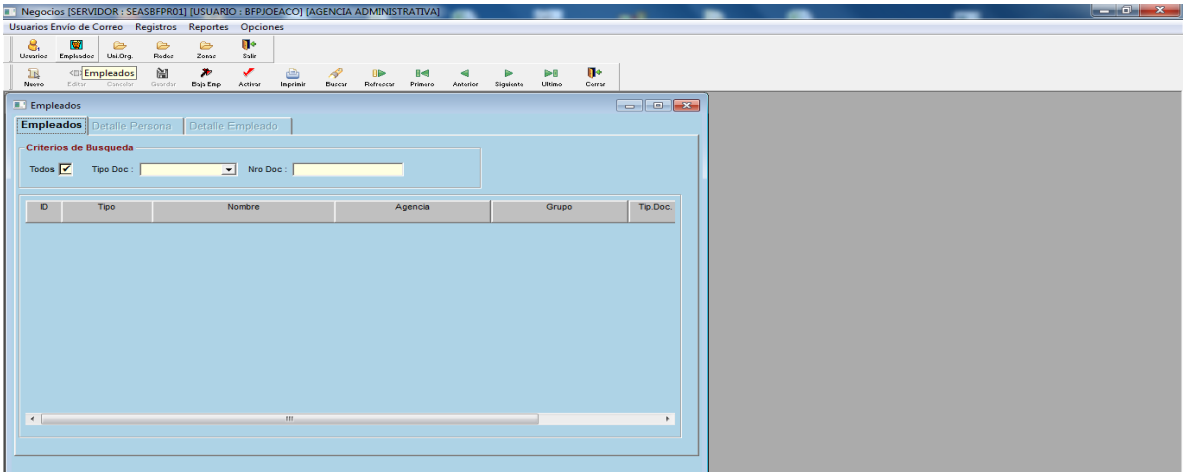
PROCESO 3.- MANTENIMIENTO DE USUARIOS EN SISTEMA MICROFINANZAS

Para el caso del sistema Microfinanzas, seguiremos el mismo enfoque planteado en los casos anteriores. Este sistema está desarrollado en Visual Basic y tiene una Base de Datos SQL Server. Se creará una Sentencia en SQL, que tenga como input nuestro archivo centralizado: **Proceso_Ceses_BFP** y tomando como atributo estandarizado ‘’Initial’’, se iniciará la baja masiva de los usuarios.

Figura N° 54 : Pantalla de Login del Sistema Microfinanzas

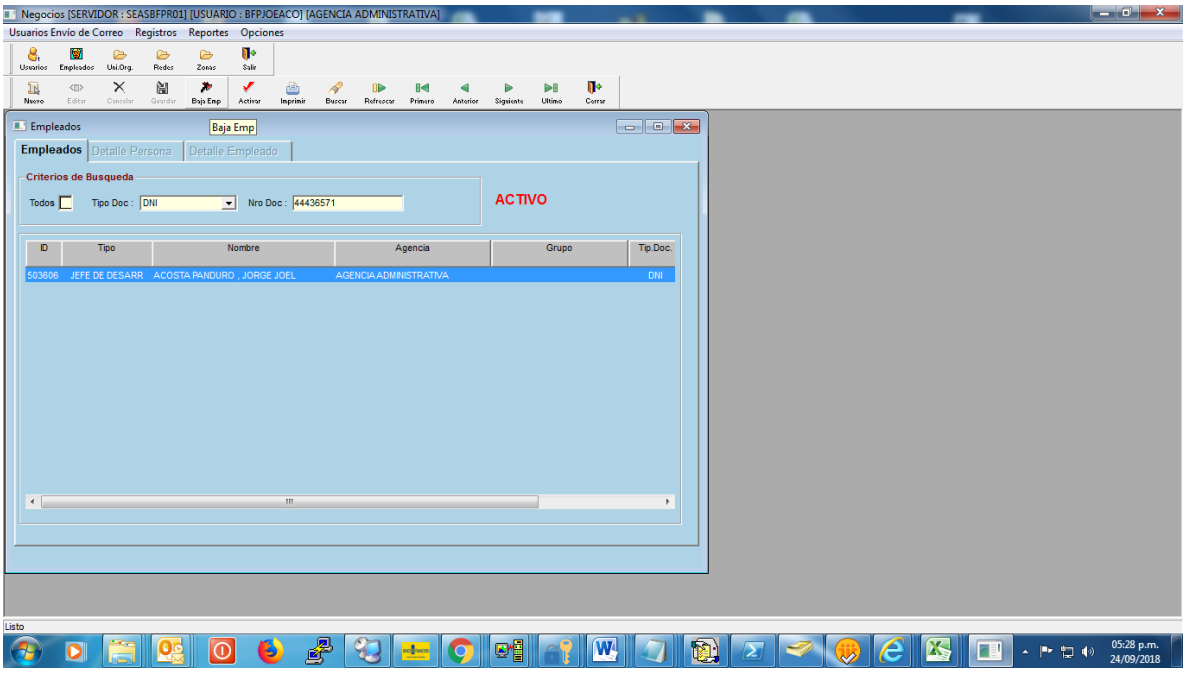
Fuente: Elaboración Propia

Figura N° 55 : Modulo de Registro Empleados



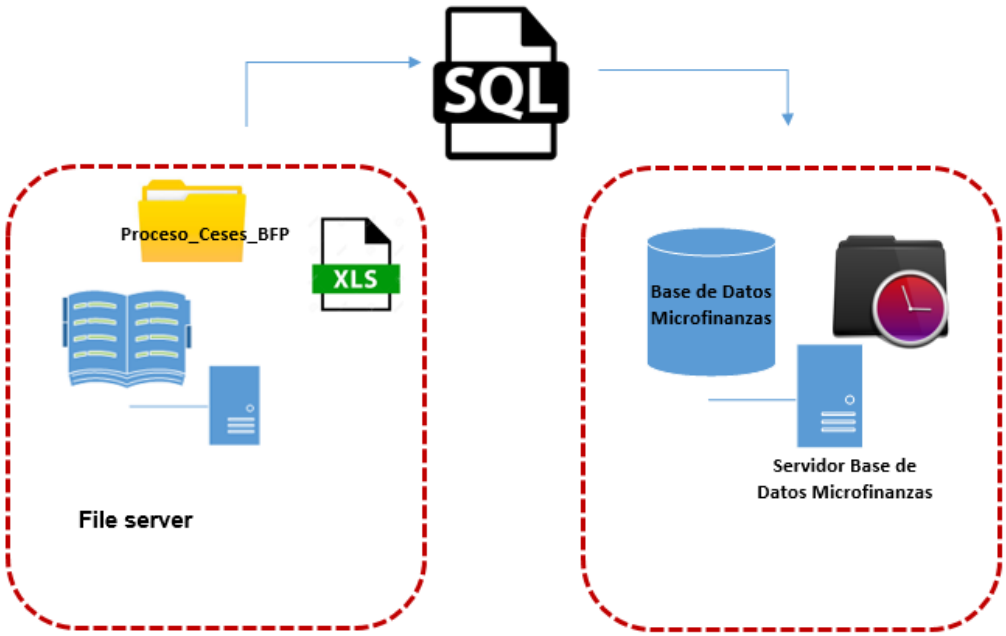
Fuente: Elaboración Propia

Figura N° 56 : Búsqueda de Empleado



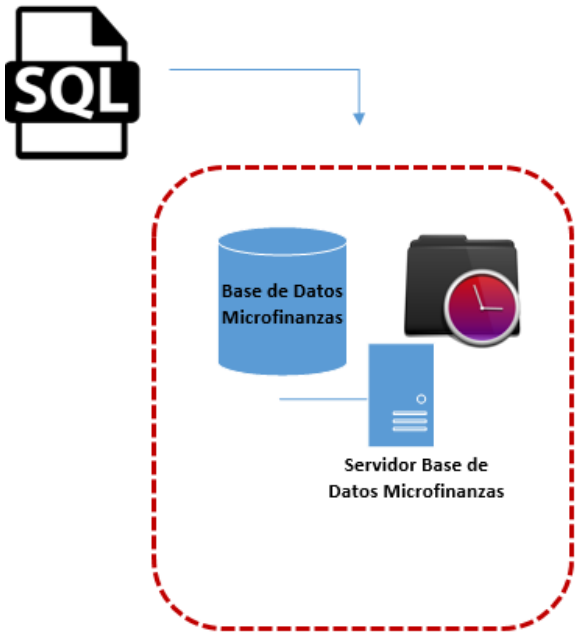
Fuente: Elaboración Propia

Figura N° 57 : Arquitectura Automatizada de Ceses Microfinanzas



Fuente: Elaboración Propia

Figura N° 58 : Tarea Programada que Ejecuta Programa SQL



Fuente: Elaboración Propia

Referencialmente la Tabla de Usuarios del sistema Microfinanzas tendría la siguiente estructura:

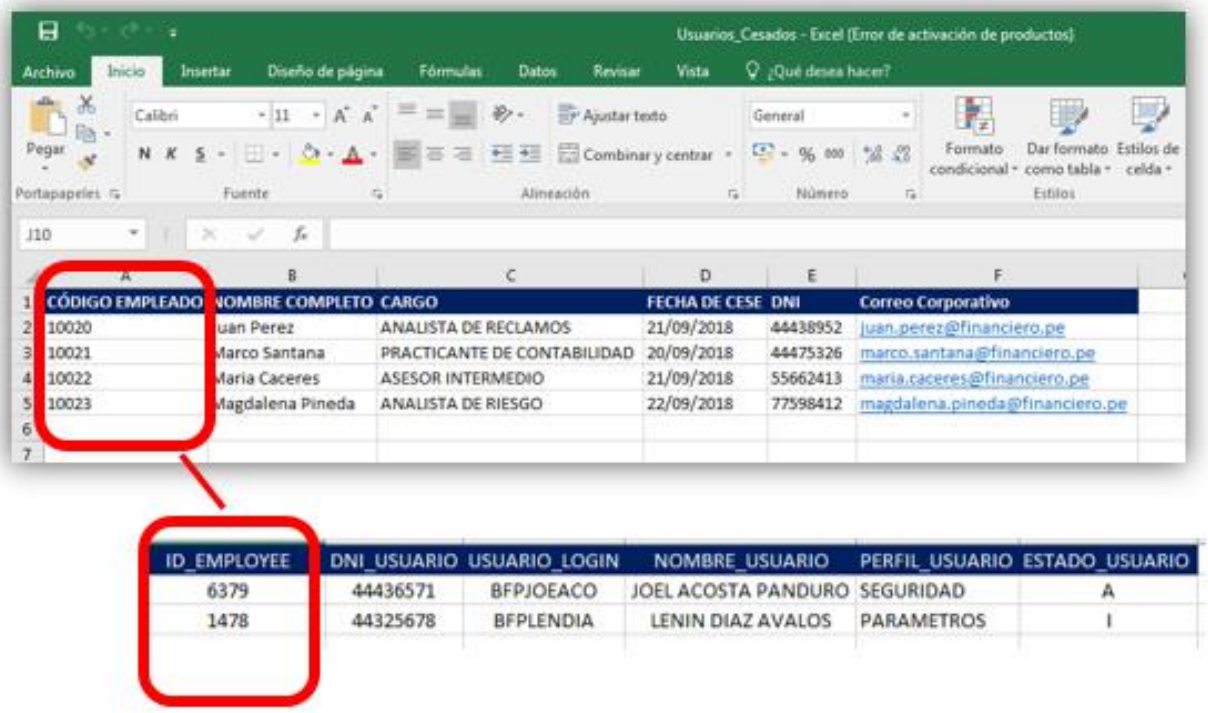
Figura N° 59 : Estructura de Datos de Tabla Usuarios

	NUMERO_REGISTRO	ID_EMPLOYEE	DNI_USUARIO	USUARIO_LOGIN	NOMBRE_USUARIO	PERFIL_USUARIO	ESTADO_USUARIO
2	1	6379	44436571	BFPJOEACO	JOEL ACOSTA PANDURO	SEGURIDAD	A
3	2	1478	44325678	BFPLENDIA	LENIN DIAZ AVALOS	PARAMETROS	I

Fuente: Elaboración Propia

Se diseñará la programación en SQL para que a través del archivo centralizado en el File Server, el Query lea archivo Excel, importe el campo CODIGO EMPLEADO y haga el match con el campo ID_EMPLOYEE donde se registra en la Base de Datos.

Figura N° 60 : Campo Importado de Archivo Excel Match Campo BD



Fuente: Elaboración Propia

La codificacion SQL sería de la siguiente forma:

Figura N° 61 : Codificación Sentencia SQL Microfinanzas

Update **Nombre_Tabla_Usuarios**

Set **ESTADO_USUARIO** = ''I'' where **DNI_USUARIO** = **DNI** desde archivo de Origen Archivo Excel

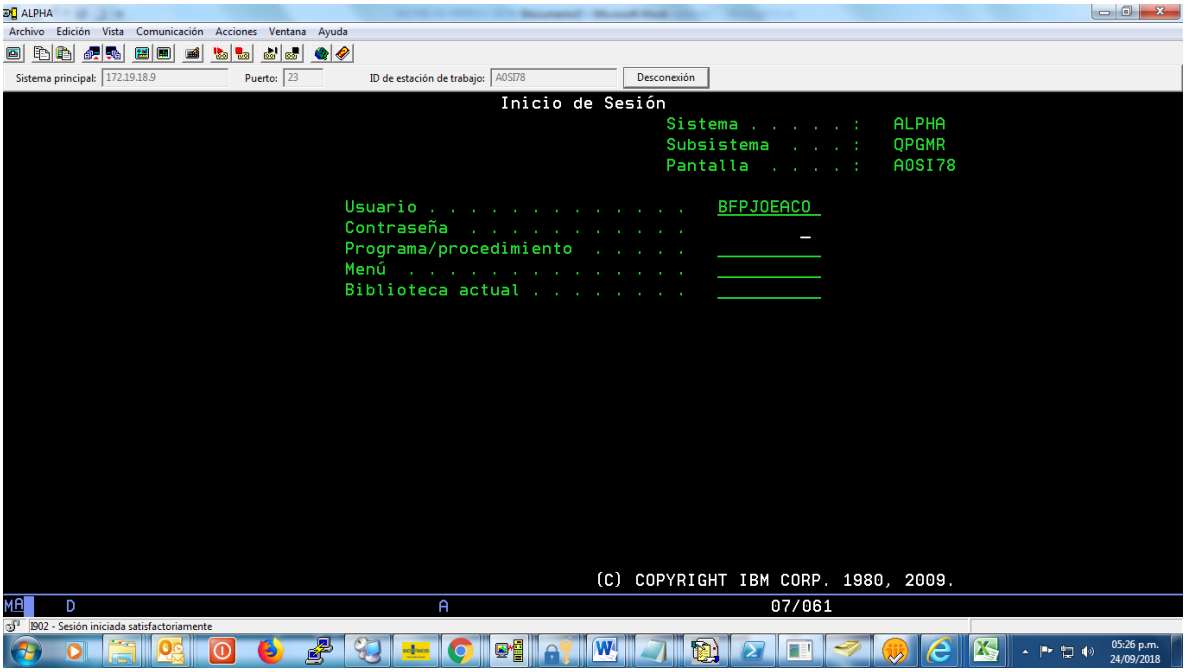
Fuente: Elaboración Propia

PROCESO 4.- MANTENIMIENTO DE USUARIOS IBS

El IBS es el programa Core del Banco Financiero, por donde pasan las consultas, operaciones y transacciones de los clientes, es por ello que es considerada una aplicación crítica la cual debe ser deshabilitada de forma inmediata apenas es recibido el Cese.

El IBS está desarrollado en RPG [1](Report Program Generator) y utiliza una Base de Datos DB2 [2] .

Figura N° 62 : Pantalla de Login en IBS

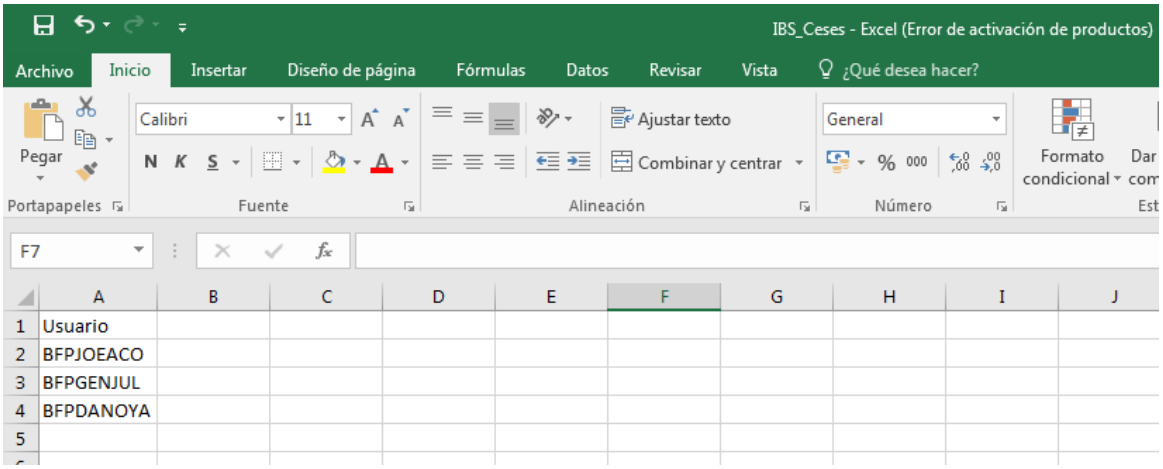


Fuente: Elaboración Propia

Para el mantenimiento de Ceses de usuarios creados en IBS, se plantea utilizar la automatización en base a la Programación que está siendo usada como piloto, pero para la actividad de Activar cuentas.

Esta programación está basada en C# y utiliza comandos que trabajan con coordenadas, lo que permite que un Robot ejecute las tareas manuales que actualmente son ejecutadas por el Analista de Control de Accesos. En este modelo existe una limitante y es que el programa necesita como input un archivo con el siguiente formato:

Figura N° 63 : Formato de Archivo Input Robot IBS



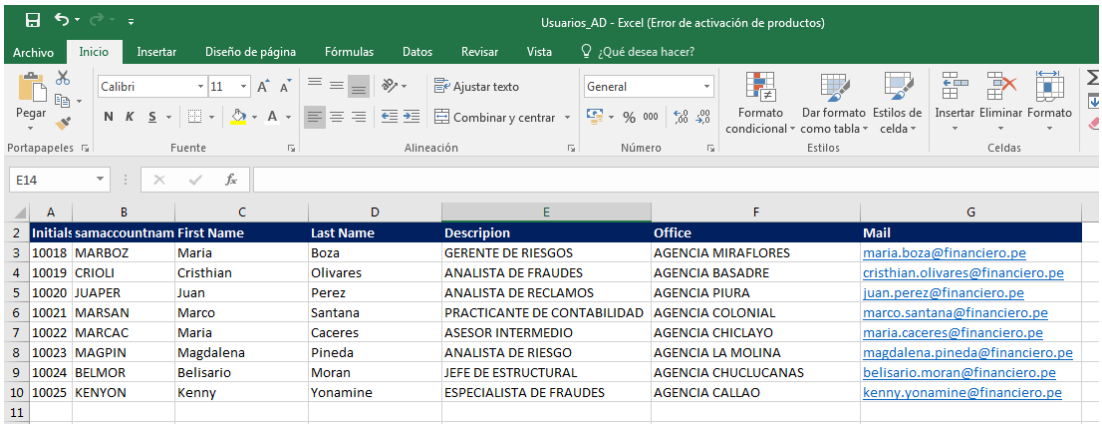
Fuente: Elaboración Propia

El archivo debe contener las cuentas creadas en el sistema IBS, sin embargo, ese dato no está incluido en la notificación de Ceses que envía Gestión de Personas:

Entonces debemos construir este archivo, para ello utilizaremos la programación de un Robot que permita cruzar la BD enviada por Gestión de Personas y el reporte de Usuarios del active Directory

La idea es que el archivo **Usuarios_Cesados** que es depositado por Gestión de Personas en repositorio centralizado se cruce con el reporte de Usuarios del Active Directory **Usuarios_AD;**

Figura N° 64 : Formato Reporte de Usuarios Active Directory

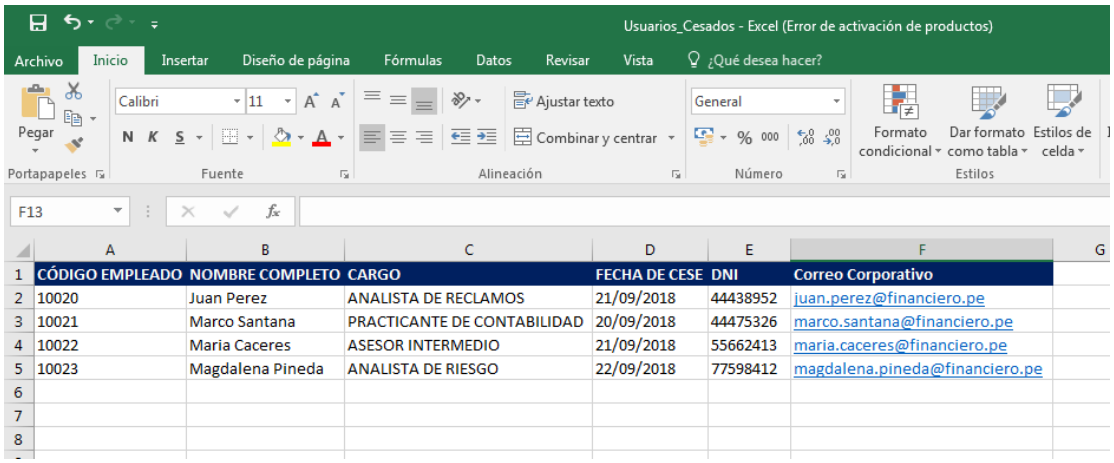


Usuarios_AD - Excel (Error de activación de productos)

	A	B	C	D	E	F	G
2	Initials	samaccountnam	First Name	Last Name	Descripion	Office	Mail
3	10018	MARBOZ	Maria	Boza	GERENTE DE RIESGOS	AGENCIA MIRAFLORES	maria.boza@financiero.pe
4	10019	CRIOLI	Cristhian	Olivares	ANALISTA DE FRAUDES	AGENCIA BASADRE	cristhian.olivares@financiero.pe
5	10020	JUAPER	Juan	Perez	ANALISTA DE RECLAMOS	AGENCIA PIURA	juan.perez@financiero.pe
6	10021	MARSAN	Marco	Santana	PRACTICANTE DE CONTABILIDAD	AGENCIA COLONIAL	marco.santana@financiero.pe
7	10022	MARCAC	Maria	Caceres	ASESOR INTERMEDIO	AGENCIA CHICLAYO	maria.caceres@financiero.pe
8	10023	MAGPIN	Magdalena	Pineda	ANALISTA DE RIESGO	AGENCIA LA MOLINA	magdalena.pineda@financiero.pe
9	10024	BELMOR	Belisario	Moran	JEFE DE ESTRUCTURAL	AGENCIA CHUCLUCANAS	belisario.moran@financiero.pe
10	10025	KENYON	Kenny	Yonamine	ESPECIALISTA DE FRAUDES	AGENCIA CALLAO	kenny.yonamine@financiero.pe
11							

Fuente: Elaboración Propia

Figura N° 65 : Archivo Depositado en Ruta Compartida



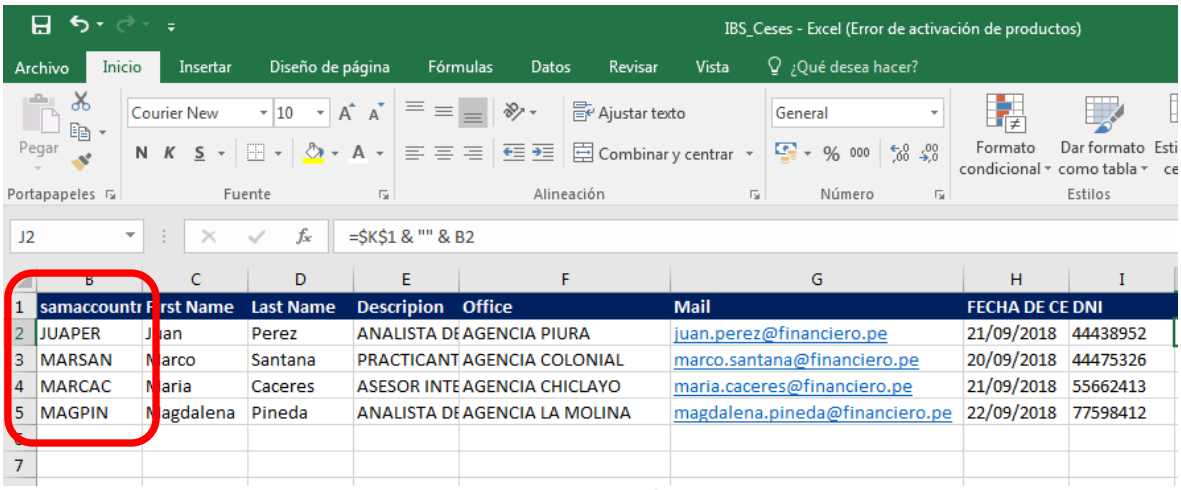
Usuarios_Cesados - Excel (Error de activación de productos)

	A	B	C	D	E	F	G
1	CÓDIGO EMPLEADO	NOMBRE COMPLETO	CARGO	FECHA DE CESE	DNI	Correo Corporativo	
2	10020	Juan Perez	ANALISTA DE RECLAMOS	21/09/2018	44438952	juan.perez@financiero.pe	
3	10021	Marco Santana	PRACTICANTE DE CONTABILIDAD	20/09/2018	44475326	marco.santana@financiero.pe	
4	10022	Maria Caceres	ASESOR INTERMEDIO	21/09/2018	55662413	maria.caceres@financiero.pe	
5	10023	Magdalena Pineda	ANALISTA DE RIESGO	22/09/2018	77598412	magdalena.pineda@financiero.pe	
6							
7							
8							

Fuente: Elaboración Propia

Lo que queremos con este match de BD de usuarios en Excel , es obtener un tercer archivo que contenga la información de los usuarios que deben ser cesados + el usuario de red ‘’**samaccountname**’’ que es un campo no considerado por Gestión de Personas .De esta forma el archivo generado sería

Figura N° 66 : Archivo Final con Campo samaccountname



	B	C	D	E	F	G	H	I
1	samaccountn	First Name	Last Name	Descripion	Office	Mail	FECHA DE CE	DNI
2	JUAPER	Juan	Perez	ANALISTA DE	AGENCIA PIURA	juan.perez@financiero.pe	21/09/2018	44438952
3	MARSAN	Marco	Santana	PRACTICANT	AGENCIA COLONIAL	marco.santana@financiero.pe	20/09/2018	44475326
4	MARCAC	Maria	Caceres	ASESOR INTE	AGENCIA CHICLAYO	maria.caceres@financiero.pe	21/09/2018	55662413
5	MAGPIN	Magdalena	Pineda	ANALISTA DE	AGENCIA LA MOLINA	magdalena.pineda@financiero.pe	22/09/2018	77598412
7								

Fuente: Elaboración Propia

Luego para Obtener el campo Usuario IBS, utilizaremos la siguiente fórmula para concatenar las celdas:

K : Corresponde a un Dato estático ‘’BFP’’

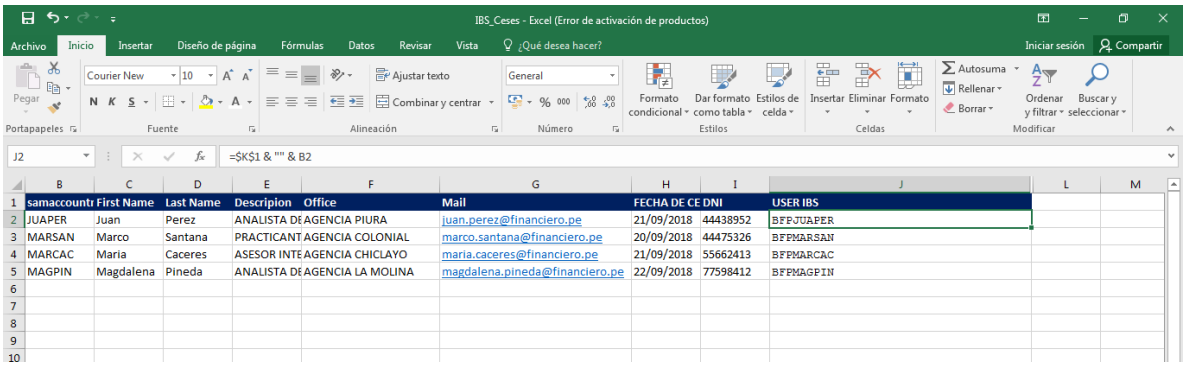
Figura N° 67 : Formula Configurada en Archivo Excel

=K1 & "" & B2

Fuente: Elaboración Propia

Obteniéndose el siguiente reporte de usuarios, en donde tenemos identificado la cuenta de IBS

Figura N° 68 : Archivo con Campo User IBS

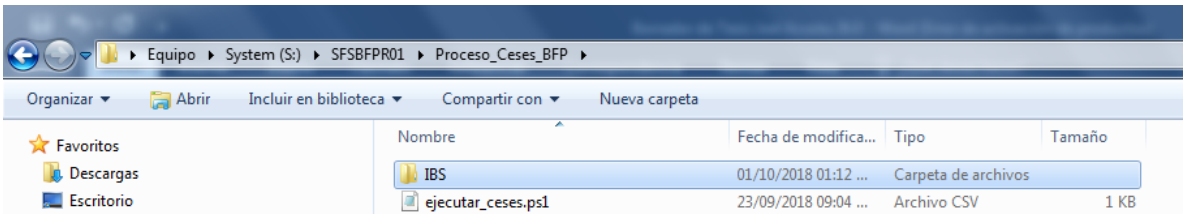


	samaccountn	First Name	Last Name	Descripion	Office	Mail	FECHA DE CE	DNI	USER IBS
2	JUAPER	Juan	Perez	ANALISTA DE	AGENCIA PIURA	juan.perez@financiero.pe	21/09/2018	44438952	BFPJUAPER
3	MARSAN	Marco	Santana	PRACTICANT	AGENCIA COLONIAL	marco.santana@financiero.pe	20/09/2018	44475326	BFPMARSAN
4	MARCAC	Maria	Caceres	ASESOR INTE	AGENCIA CHICLAYO	maria.caceres@financiero.pe	21/09/2018	55662413	BFPMARCAC
5	MAGPIN	Magdalena	Pineda	ANALISTA DE	AGENCIA LA MOLINA	magdalena.pineda@financiero.pe	22/09/2018	77598412	BFPMAGPIN

Fuente: Elaboración Propia

Este nuevo archivo, lo guardaremos en una nueva carpeta creada:

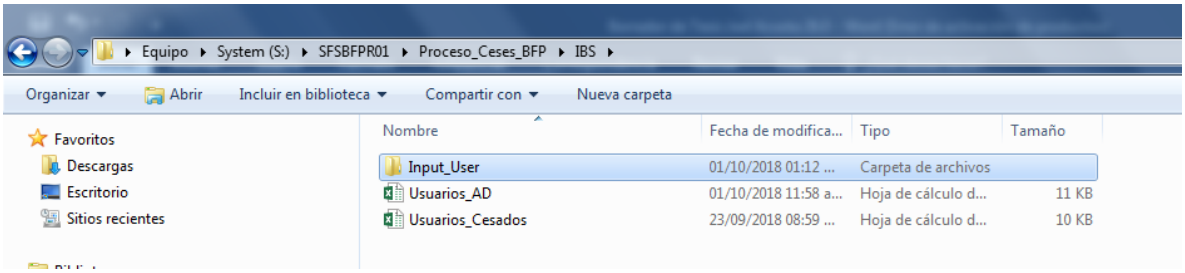
Figura N° 69 : Directorio IBS Centralizado



Fuente: Elaboración Propia

Se crea una nueva carpeta denominada **Input_User** donde se deposita el nuevo archivo que ya fue cruzado entre ambos reportes.

Figura N° 70 : Carpeta Archivo Input Robot IBS



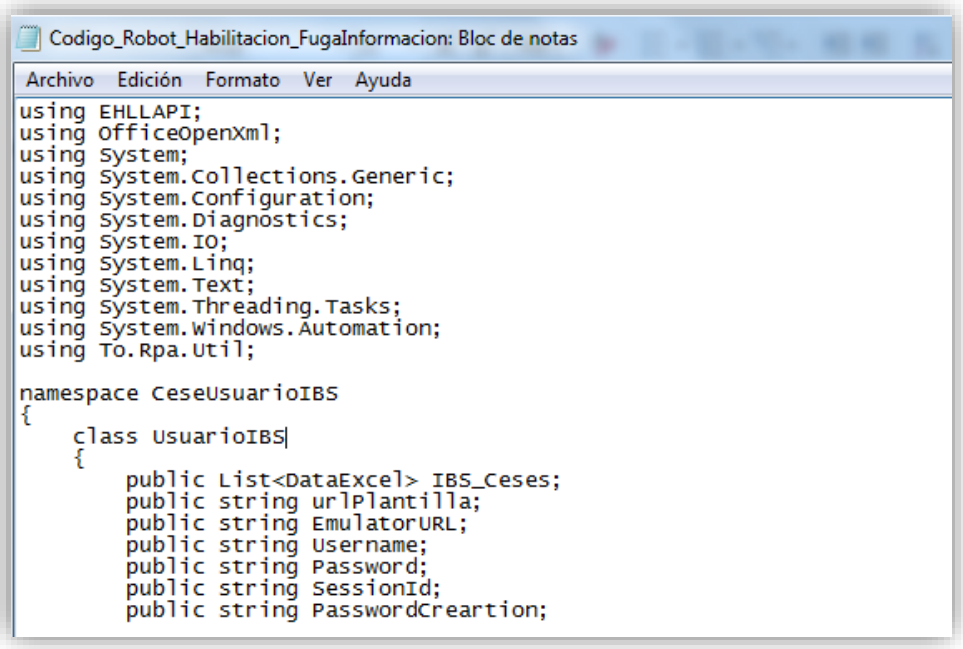
Fuente: Elaboración Propia

Desde este directorio es donde basaremos nuestra programación para el Cese de usuarios IBS. Como ya lo habíamos planteado, la automatización será programada en lenguaje C# .

[3]La estructura de la Programación sería de la siguiente forma:

En esta parte de la programación estamos asignando a las variables las credenciales de una cuenta administradora del IBS.

Figura N° 71 : Programación referencial en C# Robot IBS

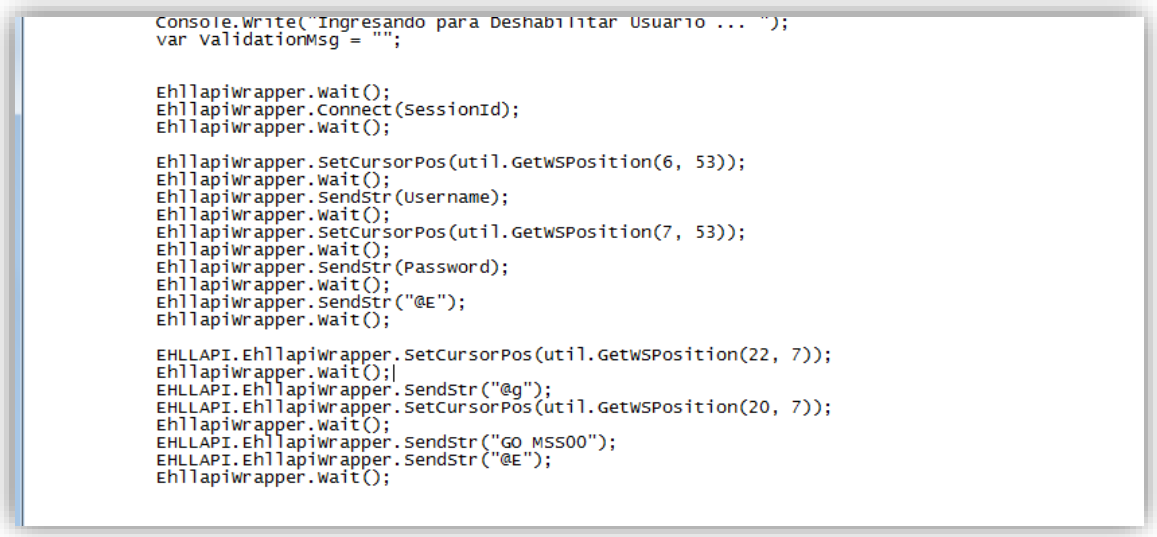


Fuente: Elaboración Propia

Aquí podemos observar como la programación trabaja en Base a Coordenadas:

[3] EHLLAPI (Interfaz de programación de aplicaciones de lenguaje de alto nivel ampliado) es una biblioteca estándar para crear interfaces para aplicaciones AS400

Figura N° 72 : Programación en Base a Coordenadas C#



```
Console.Write("Ingresando para Deshabilitar Usuario ... ");
var validationMsg = "";


EhllapiWrapper.Wait();
EhllapiWrapper.Connect(SessionId);
EhllapiWrapper.Wait();

EhllapiWrapper.SetCursorPos(util.GetWSPosition(6, 53));
EhllapiWrapper.Wait();
EhllapiWrapper.SendStr(Username);
EhllapiWrapper.Wait();
EhllapiWrapper.SetCursorPos(util.GetWSPosition(7, 53));
EhllapiWrapper.Wait();
EhllapiWrapper.SendStr(Password);
EhllapiWrapper.Wait();
EhllapiWrapper.SendStr("@E");
EhllapiWrapper.Wait();

EHLLAPI.EhllapiWrapper.SetCursorPos(util.GetWSPosition(22, 7));
EhllapiWrapper.Wait();
EHLLAPI.EhllapiWrapper.SendStr("@g");
EHLLAPI.EhllapiWrapper.SetCursorPos(util.GetWSPosition(20, 7));
EhllapiWrapper.Wait();
EHLLAPI.EhllapiWrapper.SendStr("GO MSS00");
EHLLAPI.EhllapiWrapper.SendStr("@E");
EhllapiWrapper.Wait();
```

Fuente: Elaboración Propia

3.3. PROCESO DE CESES BAJO EL NUEVO DISEÑO

En la fase anterior hemos rediseñado el mantenimiento de Usuarios en el Proceso de Ceses para el Banco Financiero, este nuevo Proceso incluye tanto la estandarización de la información inicial que será enviada por Gestión de Personas y la automatización de las tareas que involucran el Cese de un usuario en cada módulo de seguridad de las aplicaciones críticas.

En esta Fase, vamos a utilizar las siguientes herramientas para poder calcular los nuevos valores de las variables que se declararon en la presente investigación:

1. **Juicio Experto. -** Se utilizará para poder estimar el tiempo que se invertirá bajo el nuevo diseño del Proceso, en cada una de las actividades que forman parte del Flujo.

2. **Cuestionario a Expertos.** – Se aplicará un nuevo cuestionario a la misma muestra planteada en la Fase 1 , sin embargo las preguntas estarán centradas al Nivel de Riesgo asociada pero conociendo el nuevo diseño del Proceso , por lo cual los valores de la Relevancia e Impacto no variarán .

Tomamos como referencia los valores calculados en la Fase 1:

CALCULO ESFUERZO POR CESE DE USUARIO

PROCESO DE CESES ACTUAL

1. Cantidad Promedio de Ceses Diarios: **2.971 Usuarios**
2. Tiempo Promedio de Ejecución de Cese Diario: **0.42 Horas**

Tabla N° 19 : Esfuerzo Actual Aplicaciones Criticas

Sistema	Actividad en el Sistema	Modo	Esfuerzo Minutos
RED	Baja de Usuario	Manual	3
CORREO	Baja de Usuario	Manual	3
IBS	Baja de Usuario	Manual	3
MICROFINANZAS	Baja de Usuario	Manual	5
CA SERVICE DESK	Registro deTicket	Manual	5
GRP	Notificación de involucrados del Proceso	Manual	3
BD CESES	Registro de usuarios Cesados	Manual	3
TOTAL MINUTOS			**25 minutos**
TOTAL HORAS			**0.42 horas**

Fuente: Elaboración Propia

NUEVO DISEÑO DEL PROCESO DE CESE DE USUARIOS

Para calcular el Tiempo estimado de la actividad utilizaremos el método PERT que utiliza 3 estimaciones para delimitar un rango que se aproxime al tiempo de duración de una actividad:

• **Más probable (tM).** Esta estimación se basa en la duración de la actividad, en función de los recursos que probablemente le sean asignados, de su productividad, de las expectativas realistas de disponibilidad para la actividad, de las dependencias de otros participantes y de las interrupciones.

• **Optimista (tO).** Estima la duración de la actividad sobre la base del análisis del mejor escenario posible para esa actividad.

• **Pesimista (tP).** Estima la duración de la actividad sobre la base del análisis del peor escenario posible para esa actividad.

$$tE = \frac{\mathrm{tM} + \mathrm{tO} + \mathrm{tP}}{3}$$

RED $tE = \frac{8+4+10}{3} = 7.3\ Segundos$

CORREO $tE = \frac{8+4+10}{3} = 7.3\ Segundos$

IBS $tE = \frac{10+6+15}{3} = 10.3\ Segundos$

MICROFINANZAS $tE = \frac{8+4+10}{3} = 7.3\ Segundos$

Tabla N° 20 : Esfuerzo Bajo Nuevo Diseño Aplicaciones Criticas

Sistema	Actividad en el Sistema	Modo	tE Segundos	tE Minutos
RED	Baja de Usuario	Automatizado	7.3	0.12
CORREO	Baja de Usuario	Automatizado	7.3	0.12
IBS	Baja de Usuario	Automatizado	10.3	0.17
MICROFINANZAS	Baja de Usuario	Automatizado	7.3	0.12
CA SERVICE DESK	Registro deTicket	Manual	300	5
GRP	Notificación de involucrados del Proceso	Manual	180	3
BD CESES	Registro de usuarios Cesados	Manual	180	3
TOTAL MINUTOS				**11.53**
TOTAL HORAS				**0.19**

Fuente: Elaboración Propia

Tabla N° 21 ; Comparación de Esfuerzo Proceso Actual - Nuevo Diseño

ESFUERZO INVERTIDO EN 1 CESE	
PROCESO CESE ANTIGUO	**NUEVO DISEÑO DE PROCESO CESE**
0.42 horas	0.19 Horas

Fuente: Elaboración Propia

CALCULO DE CARGA OPERATIVA

PROCESO DE CESE ACTUAL

$$\boldsymbol{Carga\ Operativa\ Diaria} = \text{Cantidad Promecio Ceses x Tiempo Promedio Ceses}$$

$$\boldsymbol{Carga\ Operativa\ Diaria} = 2.971 * 0.42$$

$$\boldsymbol{Carga\ Operativa\ Diaria} = 1.25\ \text{Horas}/Hombre$$

NUEVO DISEÑO DEL PROCESO DE CESE DE USUARIOS

$$\boldsymbol{Carga\ Operativa\ Diaria} = \text{Cantidad Promecio Ceses x Tiempo Promedio Ceses}$$

$$\boldsymbol{Carga\ Operativa\ Diaria} = 2.971 * 0.19$$

$$\boldsymbol{Carga\ Operativa\ Diaria} = 0.56\ \text{Horas}/Hombre$$

Tabla N° 22 : Comparaciones fuerzo Carga Operativa

ESFUERZO CARGA OPERATIVA DIARIA	
PROCESO CESE ANTIGUO	**NUEVO DISEÑO DE PROCESO CESE**
1.25 horas	0.56 horas

Fuente: Elaboración Propia

CALCULO DE RIESGO DE FUGA DE INFORMACION

Se elaboró un nuevo cuestionario, considerando que el nuevo diseño estuviera implementado y se distribuyó a la muestra considerada para el cálculo del riesgo actual.

En este cálculo los valores de la relevancia e Impacto no variaran y nos concentraremos en el cálculo de la Probabilidad de ocurrencia del Riesgo:

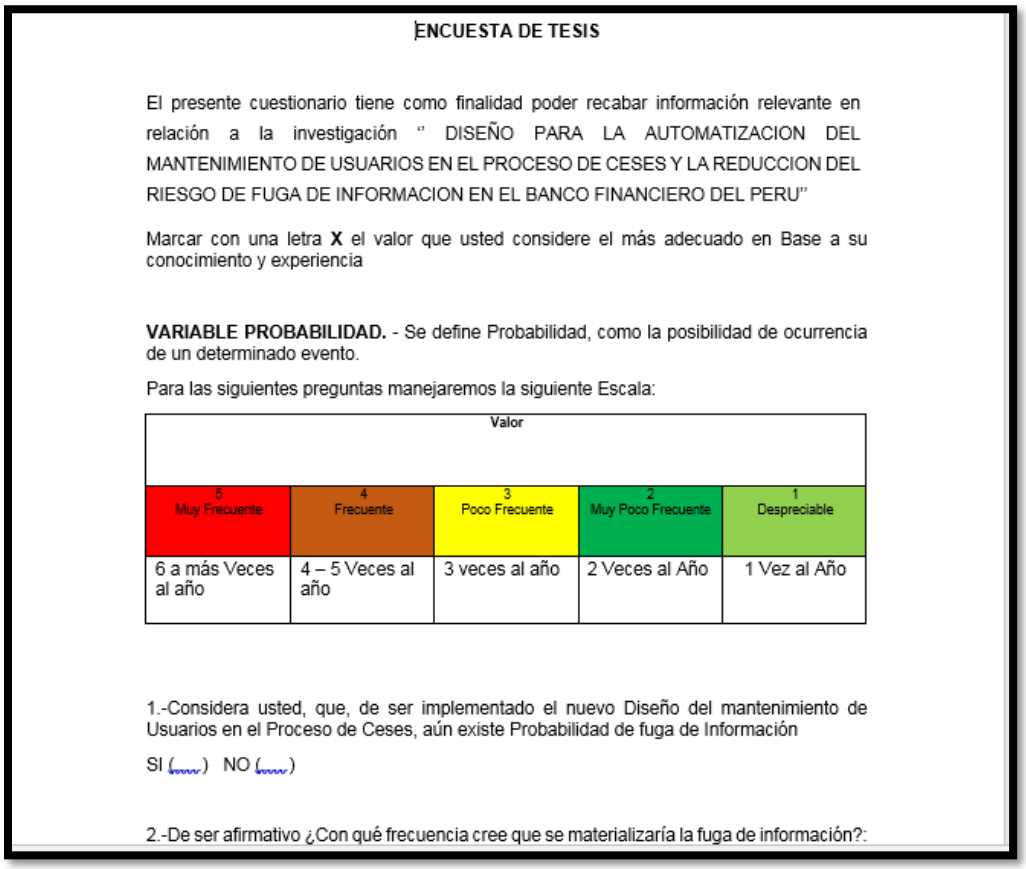
.

Riesgo=P*S*R

Riesgo=P*4.30*4.66

A continuación, se muestran los resultados del cuestionario entregado a los usuarios de la muestra. A la pregunta:

Figura N° 73 : Cuestionario 2



ENCUESTA DE TESIS

El presente cuestionario tiene como finalidad poder recabar información relevante en relación a la investigación '' DISEÑO PARA LA AUTOMATIZACION DEL MANTENIMIENTO DE USUARIOS EN EL PROCESO DE CESES Y LA REDUCCION DEL RIESGO DE FUGA DE INFORMACION EN EL BANCO FINANCIERO DEL PERU''

Marcar con una letra **X** el valor que usted considere el más adecuado en Base a su conocimiento y experiencia

VARIABLE PROBABILIDAD. - Se define Probabilidad, como la posibilidad de ocurrencia de un determinado evento.

Para las siguientes preguntas manejaremos la siguiente Escala:

Valor				
5 Muy Frecuente	4 Frecuente	3 Poco Frecuente	2 Muy Poco Frecuente	1 Despreciable
6 a más Veces al año	4 – 5 Veces al año	3 veces al año	2 Veces al Año	1 Vez al Año

1.-Considera usted, que, de ser implementado el nuevo Diseño del mantenimiento de Usuarios en el Proceso de Ceses, aún existe Probabilidad de fuga de Información

SI (.....) NO (.....)

2.-De ser afirmativo ¿Con qué frecuencia cree que se materializaría la fuga de información?:

Fuente: Elaboración Propia

1.-Considera usted, que, de ser implementado el nuevo Diseño del mantenimiento de Usuarios en el Proceso de Ceses, aún existe Probabilidad de fuga de Información

Tabla N° 23 : Resultados de Cuestionario 2

Usuario	SI	NO
1	X	
2	X	
3	X	
4	X	
5	X	
6	X	
7	X	
8	X	
9	X	
10	X	
11	X	
12	X	
13	X	
14	X	
15	X	
16	X	
17	X	
18	X	
19	X	
20	X	
21	X	
22	X	
23	X	
24	X	
25	X	
26	X	
27	X	
28	X	
29	X	
30	X	

Fuente: Elaboración Propia

A pesar de implementar el nuevo diseño del mantenimiento de usuarios en el Proceso de Ceses, los 30 encuestados creen que existe probabilidad de fuga de información

A la pregunta: De ser afirmativa la pregunta 1 **¿Con qué frecuencia cree que se materializaría la fuga de información?:**

Tabla N° 24 : Resultados de Pregunta 2 Cuestionario 2

Usuario	Frecuencia Anual
1	1
2	2
3	2
4	1
5	2
6	2
7	1
8	1
9	2
10	1
11	1
12	2
13	1
14	2
15	1
16	1
17	1
18	1
19	2
20	2
21	2
22	1
23	1
24	2
25	2
26	1
27	1
28	2
29	1
30	1
Promedio	1.433333333

Fuente: Elaboración Propia

Tenemos una Probabilidad Promedio: 1.43

Con el valor de la Probabilidad Promedio calculado, procedemos a calcular el nuevo nivel de Riesgo asociado:

$$Riesgo=P*4.30*4.66$$

$$Riesgo=1.43*4.30*4.66$$

$$Riesgo=28.65$$

Con el valor obtenido, lo comparamos con nuestra Matriz de Nivel de Riesgo:

Tabla N° 25 : Nuevo Nivel de Riesgo bajo Nuevo Diseño

Nivel de Riesgo de Control PSR		Acciones a Tomar
Nivel de Riesgo	Rango de Valores P*S*R	
Muy Bajo	1, 2, 3, 4, 5, 6	Son riesgos aceptables y deben ser informados para los Propietarios de los activos
Bajo	8, 9, 10, 12, 15, 16	Son riesgos que pueden ser aceptables después de revisión y confirmación de los Propietarios de los activos.
Medio	**18, 20, 24, 25, 27, 30**	**Son riesgos que pueden ser aceptables después de la revisión y confirmación de los Propietarios de los activos, todavía la aceptación del riesgo debe ser hecha por medios formales.**
Alto	32, 36, 40, 45, 48, 50	Son riesgos inaceptables y los Propietarios de los activos deben ser orientados para que por lo menos sean controlados.
Muy Alto	60, 64, 75, 80, 100, 125	Son riesgos inaceptables y los Propietarios de los activos deben ser orientados para que los mitiguen inmediatamente.

Fuente: Elaboración Propia

El nivel de Riesgo a disminuido:

Tabla N° 26 : Comparación de Nivel de Riesgo

NIVEL DE RIESGO	
PROCESO CESE ANTIGUO	**NUEVO DISEÑO DE PROCESO CESE**
77.34 Riesgo Muy Alto	28.65 Riesgo Medio

Fuente: Elaboración Propia

CALCULO DE ERRORES MANUALES

PROCESO ACTUAL

$$\%\ \boldsymbol{Errores\ Manuales} = \frac{\text{Cantidad de Usuarios con accesos a la aplicacion no Cesados}}{\text{Cantidad de Usuarios con accesos a la aplicacion}}$$

$$\%\ \boldsymbol{Efectividad} = 1 - \ \%\ Errores\ Manuales$$

Tabla N° 27 : Resumen de % Efectividad Proceso Actual

SISTEMA	% *Errores Manuales*	% *Efectividad*
RED	5	95
CORREO	5	95
IBS	2	98
MICROFINANZAS	4	96

Fuente: Elaboración Propia

Tabla N° 28 : Promedio de % Errores Manuales Proceso Actual

SISTEMA	% *Errores Manuales*
RED	5
CORREO	5
IBS	2
MICROFINANZAS	4
Promedio	4

Fuente: Elaboración Propia

NUEVO PROCESO DE CESES

Al tener automatizado el proceso de Ceses, se estima que el error manual debe ser 0 %. Esta precisión será corroborada luego del pase a producción del nuevo diseño del Proceso de Ceses.

Tabla N° 29 : Resumen % Errores Manuales Nuevo Diseño Proceso

SISTEMA	% *Errores Manuales*	% *Efectividad*
RED	0	100%
CORREO	0	100%
IBS	0	100%
MICROFINANZAS	0	100%

Fuente: Elaboración Propia

Tabla N° 30 : Comparación de % Errores Manuales

ERROR MANUAL	
PROCESO CESE ANTIGUO	**NUEVO DISEÑO DE PROCESO CESE**
4 %	0 %

Fuente: Elaboración Propia

CAPITULO 4

ANALISIS DE COSTO Y BENEFICIO

4.1.- DETERMINACION DE LOS COSTOS

En esta sección se realizará el cálculo estimado de los costos asociados, el cual estará diferenciado por las siguientes categorías:

4.1.1. Costos de Inversión:

1.1.-Costos de Personal. - Este Categoría engloba todos los gastos que estén asociados al Recurso Humano que participará en el Proyecto.

Tabla N° 31 : Costos de Personal

Recursos Humanos	Nro. Horas	Días	Horas Mensual	Cant. Meses	Pago x Hora (S/.)	Total Horas	Costo Total
Analista de Seguridad TI	3	20	60	1	S/. 20	60	S/. 1200
Analista de Desarrollo de Sistemas (Windows Server)	8	10	80	1	S/. 35	80	S/. 2800
Analista de Desarrollo de Sistemas (Lenguaje C#)	8	10	80	1	S/. 30	80	S/. 2400
Analista de Desarrollo de Sistemas (RPA)	8	20	160	1	S/. 35	160	S/. 5600
Analista de Calidad de Sistemas	3	20	40	1	S/. 30	60	S/. 1,200
Asistente de Remuneraciones	1	5	5	1	S/. 15	5	S/. 75
Jefe de Proyecto de Sistemas	5	20	100	1	S/. 40	100	S/. 4,000
TOTAL DE MONTO POR PERSONAL							**S/. 17,275**

Fuente : Elaboración Propia

1.2.-Costos Generales. - Estos costos incluyen: costos de insumos, costos de materiales y otros gastos que adicionalmente se incurran en el presente proyecto:

Tabla N° 32 : Costos Generales

Materiales a entregar al personal asignado al proyecto	Unidad de Medida	Cantidad	Precio Unitario	Total
Cuaderno	Unidad	7	S/. 3.50	S/. 24.50
Lapicero	Unidad	7	S/. 1.00	S/. 7.00
Hojas Bond	Millar	Medio	S/. 22.00	S/. 11.00
Plumones Acrílicos	Unidad	4	S/. 4.00	S/. 16.00
Pizarra Acrílica	Unidad	1	S/. 40.00	S/. 40.00
COSTO TOTAL MATERIALES				**S/. 98.50**

Fuente: Elaboración Propia

1.3.-Costos Equipos y Software. - Los costos por este concepto incluyen la categoría de equipos Informáticos y Software Licenciado.

Tabla N° 33 : Costos de Equipos

Equipos a entregar al personal asignado al proyecto	Unidad de Medida	Cantidad	Tiempo Arrendamiento	Precio Unitario	Total
Laptops HP Arrendadas **Incluye Soporte y Garantía **Incluye Sistema Operativo W7 **Incluye Paquete de Office 2013	Unidad	5	1 Mes	$/.350.00	S/. 1,750.00
COSTO TOTAL EQUIPOS					**S/. 1,750.00**

Fuente: Elaboración Propia

Tabla N° 34 : Costos de Software

Software a entregar al personal asignado al proyecto	Unidad de Medida	Cantidad	Tiempo	Precio Unitario /Anual	Total Anual	Total Mensual
Licencia DLP (Data Lost Prevention)	Unidad	5	1 Mes	S/. 175.00	S/. 875.00	S/. 72.91
Antivirus McAfee	Unidad	5	1 Mes	S/. 35.00	S/. 150.00	S/. 14.58
COSTO TOTAL SOFTWARE						**S/. 87.50**

Fuente: Elaboración Propia

4.1.2. Costos Mantenimiento:

En este concepto se incluyen todos los gastos que se incurran por revisión de la aplicación o mejoras que se planteen en la Operación durante el periodo de 1 año.

Tabla N° 35 : Costos de Mantenimiento

COSTOS DE MANTENIMIENTO	Horas Mensual	Cant. Meses	Pago x Hora (S/.)	Total Horas	Costo Total
Analista de Desarrollo de Sistemas (Windows Server)	2	12	S/. 35	24	S/. 840.00
Analista de Desarrollo de Sistemas (Lenguaje C#)	2	12	S/. 30	24	S/. 720.00
Analista de Desarrollo de Sistemas (RPA)	2	12	S/. 35	24	S/. 840.00
Analista de Calidad de Sistemas	2	12	S/. 30	24	S/. 720.00
TOTAL COSTOS DEMANTENIMIENTO					**S/. 3,120.00**

Fuente: Elaboración Propia

COSTO TOTAL DEL PROYECTO

Tabla N° 36 : Costo Total de Proyecto

COSTO DE INVERSION	
Costo de Personal	**S/. 17,275**
Costos Generales	**S/. 98.50**
Costos de Equipos	**S/. 1,750**
Costos de Software	**S/. 87.50**
Total Costos de Inversión	**S/. 19,211**
COSTO DE MANTENIMIENTO	**S/. 3,120**
Total Costos de Mantenimiento	**S/. 3,120**
TOTAL COSTO DEL PROYECTO	**S/. 22,331**

Fuente: Elaboración Propia

4.2.- ANALISIS E INTERPRETACION DE RESULTADOS

Para el siguiente análisis, consideraremos Ingresos a todos los beneficios que serán obtenidos y que devengan de la futura implementación del nuevo diseño para el mantenimiento de usuarios en el Proceso de Ceses.

Los beneficios serán calculados en Base a los siguientes puntos:

1) Ahorro de Costos por Disminución de Tiempo en el Proceso de Ceses.
2) Ahorro de Costos por Disminución De errores manuales en el Proceso.
3) Nuevos Ingresos por inversión de Tiempo de la carga Operativa de Ceses en otros Servicios.

Ahorro de Costos por Disminución de Tiempo en el Proceso de Ceses.

Tabla N° 37 : Ahorro de Costos de Personal

PROCESO CESE ANTIGUO	TIEMPO (Horas)	COSTO PERSONAL SEGURIDAD TI (Soles x horas)	COSTO DIARIO	COSTO MENSUAL (20 Días)	COSTO ANUAL
	1.25	S/. 20.00	S/. 25.00	S/. 500.00	S/. 6000.00
NUEVO DISEÑO DE PROCESO CESE	**TIEMPO (Horas)**	**COSTO PERSONAL SEGURIDAD TI (Soles)**	**COSTO DIARIO**		
	0.56	S/. 20.00	S/. 11.20	S/. 224.00	S/. 2688.00
AHORRO ANUAL					S/. 3312.00

Fuente: Elaboración Propia

Ahorro de Costos por Disminución De errores manuales en el Proceso.

Tabla N° 38 : Esfuerzo en Re trabajo

PROCESO CESE ANTIGUO	TIEMPO (Minutos)	CANTIDAD HALLAZGOS	TIEMPO RETRABAJO (Minutos)	TIEMPO RETRABAJO (Horas)
RED	3	38	114	1.9
CORREO	3	38	114	1.9
IBS	3	11	33	0.55
MICROFINANZAS	5	8	40	0.66666667
ESFUERZO TOTAL RETRABAJO				**5.02**

Fuente: Elaboración Propia

Tabla N° 39 : Costos de Re trabajo

PROCESO CESE ANTIGUO	TIEMPO RETRABAJO (Horas)	COSTO DE PERSONAL SEGURIDAD TI (Horas)	COSTO ANUAL
RED	1.9	S/. 20.00	S/. 38.00
CORREO	1.9	S/. 20.00	S/. 38.00
IBS	0.55	S/. 20.00	S/. 11.00
MICROFINANZAS	0.66666667	S/. 20.00	S/. 13.13
COSTO TOTAL RETRABAJO			**S/. 100.13**

Fuente: Elaboración Propia

Tabla N° 40 : Costos por Penalidad Incumplimiento SLA

PROCESO CESE ANTIGUO	CANTIDAD HALLAZGOS	PENALIDAD	COSTO ANUAL
RED	38	S/. 50.00	S/. 1900.00
CORREO	38	S/. 50.00	S/. 1900.00
IBS	11	S/. 50.00	S/. 550.00
MICROFINANZAS	8	S/. 50.00	S/. 400.00
COSTO TOTAL PENALIDAD			**S/. 4750.00**

Fuente: Elaboración Propia

Tabla N° 41 ; Costo Total de Errores Manuales

PROCESO CESE ANTIGUO	CANTIDAD HALLAZGOS
COSTO TOTAL RETRABAJO	S/. 100.13
COSTO TOTAL PENALIDAD	S/. 4750.00
COSTO TOTAL ERRORES MANUALES	**S/. 4850.13**

Fuente: Elaboración Propia

Tabla N° 42 : Ahorro De Costos Anual Errores Manuales

PROCESO	COSTO TOTAL ERRORES MANUALES
DISEÑO ACTUAL	S/. 4850.13
NUEVO DISEÑO	S/. 0
AHORRO ANUAL	**S/. 4850.13**

Fuente: Elaboración Propia

Nuevos Ingresos por inversión de Tiempo de la carga Operativa de Ceses en otros Servicios.

Este Calculo corresponde al ahorro que tendríamos en personal que ya no ejecutaría labores operativas en el Proceso de Cese de Usuarios.

Tabla N° 43 : Ahorro Personal Seguridad TI Nuevo Diseño

TIEMPO LIBERADO	COSTO PERSONAL SEGURIDAD TI (Soles x horas)	COSTO DIARIO	COSTO MENSUAL (20 Días)	COSTO ANUAL
0.69 Horas	S/. 20.00	S/. 13.8	S/. 276.00	S/. 3,312.00

Fuente: Elaboración Propia

Sin embargo, el tiempo que queda liberado será invertido en la atención de otros Requerimientos que demanda el Banco Financiero y que generan mayores ingresos:

Tabla N° 44 : Pago por Otros Servicios

TIEMPO LIBERADO	PAGO POR OTROS SERVICIOS	PAGO DIARIO	PAGO MENSUAL (20 Días)	PAGO ANUAL
0.69 Horas	S/. 55.00	S/. 37.95	S/. 759.00	S/. 9,108.00

Fuente: Elaboración Propia

En resumen, tenemos un Ingreso Mensual de:

Tabla N° 45 : Ingresos Versus Egresos Anuales

	INGRESOS
INGRESOS POR OTROS SERVICIOS	S/. 9,108.00
COSTO PERSONAL	S/. 3,312.00
TOTAL DE INGRESOS ANUALES	**S/. 5,796.00**

Fuente: Elaboración Propia

4.3.- FLUJO DE CAJA

En la siguiente tabla se muestra el flujo de caja del proyecto de implementación en un período de 5 años, dónde se muestra la inversión inicial, los costos y beneficios del proyecto. Finalmente, como resultado se muestra el beneficio efectivo por cada año.

Tabla N °46 : Flujo de Caja

FLUJO DE CAJA							
COSTO/BENEFICIO		**AÑOS**					
		0	**1**	**2**	**3**	**4**	**5**
Inversión Inicial **Costos (Egresos)**	**Costos de Inversión**						
	Costos de Personal	S/. 17,275					
	Costos Generales	S/. 98.50					
	Costos de Equipos	S/. 1,750.00					
	Costos de Software	S/. 87.50					
	Total Costos de Inversión	S/. 19,211	0	0	0	0	0
	Costos de Mantenimiento						
	Total Costos de Mantenimiento		S/. 3,120.00	S/. 3,120.00	S/. 3,120.00	S/. 3,120.00	S/. 3,120.00
	Total Egresos	S/. 19,211	S/. 3,120.00	S/. 3,120.00	S/. 3,120.00	S/. 3,120.00	S/. 3,120.00
Beneficios (Ingresos)	Ahorro Errores Manuales		S/. 4,850.13	S/. 4,850.13	S/. 4,850.13	S/. 4,850.13	S/. 4,850.13
	Ingreso por Otros Servicios		S/. 5,796.00	S/. 5,796.00	S/. 5,796.00	S/. 5,796.00	S/. 5,796.00
	Total Ingresos		S/. 10,646.13	S/. 10,646.13	S/. 10,646.13	S/. 10,646.13	S/. 10,646.13
BENEFICIO EFECTIVO(BENEFICIO - COSTO)		**S/. 19,211**	**S/. 7,526.13**	**S/. 7,526.13**	**S/. 7,526.13**	**S/. 7,526.13**	**S/. 7,526.13**

Fuente: Elaboración Propia

4.4.- CALCULO DEL VAN Y TIR

En esta sección vamos a calcular el VAN (**Valor Actual Neto**) que nos sirve para ratificar si la implementación del proyecto es viable en Banco Financiero del Perú. Para ello al realizar los cálculos debemos alcanzar como resultado un **VAN mayor a 0**.

El TIR (**Tasa Interna de Retorno**) será calculado para probar a qué tasa de descuento se obtendría un VAN igual a 0. Si el valor del TIR es mayor a la tasa de interés del 10% elegida para el cálculo del VAN, podremos concluir que el proyecto es rentable.

A continuación, se muestran los valores de los ingresos y egresos a ser utilizados para el cálculo de los indicadores VAN y TIR:

Tabla N° 47 : Egresos

EGRESOS	
AÑO	VALOR
1	S/. 3,120.00
2	S/. 3,120.00
3	S/. 3,120.00
4	S/. 3,120.00
5	S/. 3,120.00
TOTAL	S/. 15,600.00

Fuente: Elaboración Propia

Tabla N° 48 : Ingresos

INGRESOS	
AÑO	VALOR
1	S/. 10,646.13
2	S/. 10,646.13
3	S/. 10,646.13
4	S/. 10,646.13
5	S/. 10,646.13
TOTAL	S/. 53230.65

Fuente: Elaboración Propia

Tabla N° 49 : Efectivo Neto

FLUJO EFECTIVO NETO	
AÑO	VALOR
1	S/. 7,526.13
2	S/. 7,526.13
3	S/. 7,526.13
4	S/. 7,526.13
5	S/. 7,526.13
TOTAL	S/. 37,630.65

Fuente: Elaboración Propia

Formulación de Datos:

fn: Flujo del Periodo

n: Cantidad de Años = 5

i: Tasa de Interés 10%

io: Inversión Inicial = **S/. 19,211**

$$\mathbf{VAN} = \left(\sum_{n=1}^{n} \frac{fn}{(1+i)^{\frac{n}{}}} \right) - io$$

$$\frac{7526.13}{(1+0.10)} + \frac{7526.13}{(1+0.10)^{\frac{2}{}}} + \frac{7526.13}{(1+0.10)^{\frac{3}{}}} + \frac{7526.13}{(1+0.10)^{\frac{4}{}}} + \frac{7526.13}{(1+0.10)^{\frac{5}{}}} \text{ - S/. 19,211}$$

VAN = S/9,318.95

TIR

$$\mathbf{0} = \left(\sum_{n=1}^{n} \quad \frac{fn}{(1+i)^{\frac{n}{}}} \right) - io$$

VAN = 28%

En resumen, tenemos:

VAN = S/9,318.95 mayor a 0
TIR = 28 % mayor a la tasa 10%

De esta forma podemos concluir que el proyecto para el Nuevo Diseño del mantenimiento de usuarios en el proceso de Ceses del Banco Financiero es viable.

CONCLUSIONES

1. En la presenta investigación se ha comprobado que el nuevo Diseño de automatización para el mantenimiento de usuarios en el Proceso de Ceses del Banco Financiero es un Proyecto Viable.

2. Hemos confirmado que el Nuevo Diseño automatizado del mantenimiento de Usuarios en el Proceso de Ceses disminuye el riesgo de Fuga de información. Dado Esto se sustenta en que el nivel de riesgo asociado al Proceso Actual considerado como **Alto Riesgo** desciende a la escala de **Riesgo Medio**.

3. Hemos confirmado que el Nuevo Diseño automatizado del mantenimiento de Usuarios en el Proceso de Ceses mejora la eficiencia en la atención del servicio. Los resultados arrojan que la atención de un Cese disminuye en más del 50% del tiempo actual.

4. Hemos confirmado que el Nuevo Diseño automatizado del mantenimiento de Usuarios en el Proceso de Ceses reduce la carga Operativa del equipo Seguridad TI – Control de Accesos, con ello el tiempo que queda liberado puede invertirse en la atención de otros servicios que se prestan al Banco.

5. Hemos confirmado que el Nuevo Diseño automatizado del mantenimiento de Usuarios en el Proceso de Ceses anula los errores manuales dado que se tiene tareas programadas.

BIBLIOGRAFIA

27001 Acdemy. (2018). ¿Qué es norma ISO 27001? Obtenido de 27001 Acdemy: https://advisera.com/27001academy/es/que-es-iso-27001/

Castro Valverde Karla Evita, G. D. (2010). IMPLEMENTACION DEL SISTEMA DE ADMINISTRACION DE ACCESOS E IDENTIDADES EN EL PROCESO DE CONTROL DE ACCESOS.

Chiavenato Idalberto. (2006). Introduccion a la Teoria General de la Administracion. Mexico: McGraw-Hill Interamericana.

Comision Economica para America Latina y el Caribe. (2003). Los caminos hacia una sociedad de la información en América Latina y el Caribe. Obtenido de Comision Economica para America Latina y el Caribe: https://www.cepal.org/es/publicaciones/2354-caminos-sociedad-la-informacion-america-latina-caribe

Czinkota Michael, K. M. (2001). Administracion de Mercadotecnia. International Thomson.

ISO 2700.ES. (2012). El portal de ISO 27001 en Español. Obtenido de ISO 2700.ES: http://www.iso27000.es/iso27000.html

ISOTools. (25 de Agosto de 2016). Cómo clasificar la información según ISO 27001. Obtenido de ISOTools: https://www.isotools.com.co/clasificar-la-informacion-segun-iso-27001/

López Yepez José. (2004). Diccionario Enciclopédico de Ciencias de la Documentación. Madrid.

Martinez Cabrera Jehu Benigno, M. (2018). IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO A RED EN LA EMPRESA SIMA. Chimbote: Tesis de Grado.

Martínez de Sousa, J. (2004). Diccionario de Bibliologia y Ciencias Afines. Guijon - España: Ediciones Trea.

Mendoza Azury. (2017). Automatización de Procesos: Ventajas y desventajas. Obtenido de gbadvisors: http://www.gb-advisors.com/es/automatizacion-de-procesos/

Mijailov, A., & Guilarirvkii, A. C. (1973). Fundamentos de la Informatica. La Habana: IDICT, Academia.

NOTICEBORED. (2018). ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls (second edition). Obtenido de NOTICEBORED: http://www.iso27001security.com/html/27002.html

Olivos Guerra Frankz, G. S. (2017). FORMULACIÓN DE POLÍTICAS DE CONTROL DE ACCESOS Y SEGURIDAD FÍSICA Y DEL ENTORNO BASADO EN LA NORMA TÉCNICA PERUANA NTP-ISO/IEC 17799 PARA LA MEJORA DE LA GESTIÓN EN LA OFICINA CENTRAL DE CÓMPUTO – UNIVERSIDAD DE LAMBAYEQUE. Lambayeque: Tesis de Grado .

Ponsa Asensio, P. (. (2006). Automatización de procesos mediante la guía GEMMA. Barcelona: Universitat Politécnica de Catalunya. Iniciativa Digital Politécnica.

Real Academia Española. (2018). Diccionario de la Lengua Española. Obtenido de Diccionario de la Lengua Española: http://dle.rae.es/?id=4TTxbev
Real Academia Española. (2018). Diccionario de la Lengua Española. Obtenido de Diccionario de la Lengua Española: http://dle.rae.es/?id=4TVTwDp

SGSI Blog especializado en Sistemas de Gestión . (2018). ¿Qué es un SGSI? Obtenido de SGSI Blog especializado en Sistemas de Gestión : https://www.pmg-ssi.com/2014/01/que-es-un-sgsi/

Superintencia de Banca, S. y. (2009). CIRCULAR Nº G- 140 -2009. Lima.

van Bon, J., De Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen,, A., & Verheijen, T. (2008). Fundamentos de ITIL®, Volumen 3. Amersfort: Van Haren Publishing.